明 細 書

コンテンツ配信方法及びコンテンツサーバ

技術分野

[0001] 本発明は、コンテンツ配信方法及びコンテンツを配信するコンテンツサーバに関する。より詳細には、一般的なデジタルコンテンツに関するデジタル著作権管理(DRM)または知的財産権管理および保護(IPMP)に関し、さらに詳細には、任意のデータフォーマットによらないデジタルコンテンツの保護および管理に関する。

背景技術

[0002] さまざまな種類のネットワークが広範囲に展開されているため、CD、DVDを用いるほかに、かかるネットワークを通じて、ユーザに、デジタルコンテンツを配布および配信できることが要求される。対応する問題が、コンテンツ所有者によって提起されている。このような方法でコンテンツを販売することが安全であるのか。

[0003] ハードディスクまたは他の記憶組込み装置が一段と多くなるにつれて、別の問題は、コンテンツ保護技術が付与された権利を公正に行使することができることをいかにして保証することができるかという点にある。

[0004] さまざまなネットワークを通じて伝送することが容易になるようにデジタル形式でコンテンツをパッケージ化するために用いる多くの異なるデジタルフォーマットが存在するため、異なるデジタルフォーマットの中で保護技術をどのように相互に用いることができるかという問題が生じる。

[0005] 同時に、ユーザが豊かなユーザ体験を享受するためにかかる権利を購入する場合には、友達と共有してでも、ユーザはコンテンツを楽しむために低コストで便利というより多くの要求を持っている。

[0006] コンテンツ所有者は任意の違法コピーを心配しているため、葛藤が常にあり、折から市場に公開された保護技術がないことから、コンテンツプロバイダは独自の方法でコンテンツを保護しようとしている。

[0007] このことは、コンテンツを販売するコンテンツ所有者に対して大きな障害をもたらすのみならず、コンテンツプロバイダが用いるさまざまな保護技術にちょうど適合させる

ために異なるバージョンを製作するCE(家庭用電化製品)メーカにとっても大きなコストをもたらす。

[0008] MPEG−21は、広範囲のネットワークおよび異なる共同体によって用いられる装置間においてデジタルコンテンツの透過的かつ増大する利用を可能にするために、汎用フレームワークを定義しようとしている。ネットワークまたは装置間で用いられている場合のコンテンツの保護方法は、MPEG−21においてきわめて重要な項目となっている。この項目は、MPEG−21のパート4であり、MPEG−21 IPMP(知的財産権管理および保護)と呼ばれている。

[0009] 過去において、コンテンツがMPEG−4／2フォーマットでパッケージ化されている場合、MPEG−4／2 IPMP拡張に従事している人々は、任意のコンテンツを保護するために、MPEG−4／2システムに基づくコンテンツ保護スキームを定義する必要があった。

[0010] MPEG−21では、デジタルアイテム(DI)は、標準表現、識別および記述を有する任意のデジタルコンテンツのための構造化デジタルオブジェクトとして定義され、MPEG−21フレームワーク内の交換、配布、トランザクションの基本単位として用いられる。

[0011] デジタルアイテムは、デジタルアイテム宣言(Digital Item Declaration:DID)によってXMLを用いて宣言し、表現される。映像、音楽、画像などのMPEG−21におけるメディアリソースとして表現されるデジタルコンテンツの他に、DIDは、さまざまな種類の機能的なメタデータを含む柔構造を与える。このようなメタデータは、たとえばメディアリソースフォーマットを記述し、リソース保護スキームを指定し、リソースに識別名を与え、ユーザプリファランスを提供すると考えられる。

[0012] DID技術の中核に加えて、他の主要な技術もまた、念入りに開発されたか、または開発中である。デジタルアイテム識別(DII)、デジタルアイテム適応(DIA)、知的財産権管理および保護(IPMP)、REL(権利表現言語)／RDD(権利データ辞書)のほか、ER(イベント報告)はすべて、デジタルアイテムの用法を広範囲に活用するための重要な技術である。実際のメディアリソース消費を支援するために、これらの技術によって定義される機能的なメタデータをすべて、DID文書(DIDドキュメント)に

入れることができる。

[0013] デジタルコンテンツに対しては、不正コピー等の著作権侵害を防止するために、暗号化等の保護処理が行われる。上記DID文書において、IPMPに関する記述(以下、単に「IPMP記述」という。)は、例えば、上記保護処理を行う際に用いた保護処理ツール、又は上記保護を解除する保護解除ツールについての記述である。ユーザ側の端末は、そのIPMP記述を解析する。ユーザは、その解析結果から必要な保護解除ツールをダウンロードし、この保護解除ツールを用いてコンテンツの保護を解除することにより、そのコンテンツの再生や印刷等の処理を行う。なお、保護処理ツールと保護解除ツールは対になっているため、IPMP記述に保護処理ツールが記述されていても、それに対応する保護解除ツールをダウンロードすることは可能である。なお、保護処理ツールは、例えば、暗号化ツール、電子透かし埋め込みツール、及びデジタル署名ツール等であり、それらに対応する保護解除ツールは、それぞれ復号化ツール、検出ツール、及び照合ツールである。以下、「IPMPツール」とは、上記保護処理ツール又は保護解除ツールをいう。

[0014] また、RELは、「Johnは、1ヶ月間1つの楽曲を再生することができる」といったユーザの権利、言い換えればコンテンツの利用条件を規定する言語である。ユーザ端末は、RELの記述を解析する。ユーザは、そのREL記述によって規定された利用条件を満たしている場合にのみ、そのコンテンツの再生や印刷等の処理を行うことができる。

[0015] 図1は、従来のDID文書の一例を示す図である。図1に示されるように、DID文書1．1は、その内部に、コンテンツ又はコンテンツのアドレスを「リソース」としてもつデジタルアイテム1．6を有する。図1に示されるように、DID文書1．1は、IPMP記述(1．2)を有する。IPMP記述(1．2)には、各デジタルアイテム1．6に必要な保護解除ツールが全て記述されている。また、コンテンツの利用条件を示すREL記述(図示せず)は、そのコンテンツ又はコンテンツのアドレスを有するデジタルアイテム1．6の記述子に記述されている。

[0016] コンテンツ保護および管理機構は、市場のニーズを反映するために、特にMPEG−21ドメインの範囲において、多くの異なるアプリケーションドメインによって作成され

る要件の大部分を対処するように強く要求されることが多い。

非特許文献1:発明者:ファング・ゾンヤン(Zhongyang Huang)、ジ・ミン(Ming Ji)、シェン・シェンメイ(Shengmei Shen)、妹尾孝憲、小暮拓世、上野孝文、「MPEG−21システムの装置(Appratus of a MPEG−21 System」に関する特許、内部特許番号Pat01.028、2002年2月に日本にて出願

非特許文献2:「MPEG−21 デジタルアイテム宣言最終国際標準案(ISO/IEC 21000−2 MPEG−21 Digital Item Declaration FDIS)」、ISO/IEC JTC 1 SC29/WG11/N4813、2002年5月

非特許文献3:「MPEG−21アーキテクチャ、シナリオおよびIPMP要件(MPEG−21 Architecture, Scenarios and IPMP Requirements)」、ISO/IEC JTC 1 SC29/WG11/N5874、2003年7月

発明の開示

発明が解決しようとする課題

[0017] 従来のDID文書において、特定のコンテンツに関するIPMP記述とREL記述は、そのコンテンツ又はコンテンツのアドレスを有する同一のデジタルアイテムに一緒に記述されず、別々に記述されていた。しかし、IPMP記述とREL記述は密接不可分な関係にあるので、それらの記述を別々に解析すると、効率が悪く、時間のロスが大きいという問題があった。例えば、図1に示されるDID文書をユーザに配信した場合、ユーザ端末は、DID文書を最初の記述から順に、すなわち図1において左上、左下、右上、右下の順に解析するので、まずIPMP記述(1.2)を解析する。上述したように、このIPMP記述には、各デジタルアイテム1.6に必要な保護解除ツールが全て記述されている。ユーザ端末は、IPMP記述(1.2)によって示された全ての保護解除ツールをダウンロードし、その後、各デジタルアイテム1.6のコンテンツに関するREL記述を順次解析する。この場合、各デジタルアイテムのREL記述によっては、前もってダウンロードした特定の保護解除ツールが不要になる場合があり、その不要となった保護解除ツールをダウンロードするために費やした時間及びコストは無駄になってしまうという問題があった。

[0018] また、本発明は、以下の問題を解決することを課題とする。

[0019] MPEG−21 IPMPに関する要件が、本発明において目的とし、解決すべき問題である。

[0020] IPMP、具体的にはMPEG−21 IPMPは、記述子および記述スキームにおける知的財産の管理および保護をサポートするものとする。

[0021] IPMP、具体的にはMPEG−21 IPMPは、どこでもコンテンツを再生することができるような相互運用性を提供するものとする。

[0022] IPMP、具体的にはMPEG−21 IPMPは、装置が新たなメディアフォーマット、IPMPツールをサポートするためのアップグレードの発見、要求、入手およびサポートを動的に行うことができるものとする。

[0023] IPMP、具体的にはMPEG−21 IPMPは、言語の一部としてデジタルアイテム記述を参照し、外部のコンテンツ記述を照会する機構を提供するものとする。

[0024] IPMP、具体的にはMPEG−21 IPMPは、合成デジタルアイテムに関する表現を関連付ける機構を提供するものとする。

[0025] IPMP、具体的にはMPEG−21 IPMPは、デジタルアイテムのコンテナまたは他の集合体を参照する機構を提供するものとする。

[0026] IPMP、具体的にはMPEG−21 IPMPは、特定の表現が保護の対象になるようにフラグを立てるものとする。保護自体(必要であれば)は、デジタルアイテムとして表現を制御するIPMPシステムによって提供される。

[0027] IPMP、具体的にはMPEG−21 IPMPは、認証スキームを参照する機構を提供するものとする。

[0028] IPMP、具体的にはMPEG−21 IPMPは、IPMPがフォーマットまたはデジタルアイテムの配信チャネルによらないことを保証する機構を提供するものとする。

[0029] IPMP、具体的にはMPEG−21 IPMPは、IPMPツールおよびIPMP機能に関連する要件を明確に表現するものとする。

[0030] IPMP、具体的にはMPEG−21 IPMPは、信頼に足るIPMP実装を構築するために、IPMPツールおよびIPMP機能を識別する必要があるものとする。

[0031] IPMPツールおよびIPMP機能は、IPMP可能端末またはピアを構築するための構成部分である。また、端末またはピアはそのIPMP性能(IPMPツールおよびIPMP

機能)を開示することが可能であるものとする。これにより、通信端末またはピアが参加することを決定する前に、他の端末またはピアのIPMP性能を調べることが可能になる。

[0032] 本発明は、上記問題を解決するためになされたものであり、ユーザが効率良く、かつ時間を無駄にすることなく保護解除ツールを取得してコンテンツの再生等を行うことを可能にするコンテンツ配信方法及びコンテンツサーバを提供することを目的とする。

課題を解決するための手段

[0033] コンテンツのパッケージ化側では、

コンテンツに直接関連する権利および保護情報をすべてについて言及するために、IPMP制御グラフの概念を導入し、

コンテンツのパッケージ化および保護に用いられる権利および保護情報を包含するために、保護メタデータホルダとしてIPMP制御グラフまたはREL−IPMP制御グラフを定義し、

IPMP制御グラフまたはREL−IPMP制御グラフに権利および条件を入れ、

IPMP制御グラフまたはREL−IPMP制御グラフにコンテンツ暗号化情報を入れ、

IPMP制御グラフまたはREL−IPMP制御グラフに電子透かし情報を入れ、

IPMP制御グラフまたはREL−IPMP制御グラフに権利保護情報を入れ、

IPMP制御グラフまたはREL−IPMP制御グラフにコンテンツを暗号化するために用いられる鍵情報を入れて表示し、

IPMP制御グラフまたはREL−IPMP制御グラフ、あるいは権利、DIDまたは鍵位置によって示される任意の場所に鍵ライセンス情報を入れ、

IPMP制御グラフまたはREL−IPMP制御グラフにおいてツールIDを用いて、どのIPMPツールが暗号化、デジタル署名、電子透かしのために用いられるかを示し、

コンテンツIDまたはDIIおよびサブコンテンツIDを用いて、保護されるデジタルコンテンツまたはそのサブコンテンツに関して権利および保護を対応させ、

DIDコンテナまたは他のアプリケーションドメインの他の適切な場所にIPMP制御グラフまたはREL−IPMP制御グラフを配置する。

[0034] 端末側では、

コンテンツIDまたはサブコンテンツID、およびIPMP制御グラフまたはREL−IPMP制御グラフを検索するために、DIDを構文解析し、

記述に関連する権利および保護を検索するために、IPMP制御グラフまたはREL−IPMP制御グラフを構文解析し、

コンテンツまたは権利または他のメタデータを保護するために用いられるIPMPツールを呼び出し、

鍵データホルダから鍵情報を直接的または間接的に検索し、

保護されるライセンスマネジャから鍵ライセンスを検索し、

上記で得られた情報を用いて、保護されるコンテンツを保護されていない状態にし、

ツールIDによって示されるツールを用いて、権利の完全性を確認し、

コンテンツに組み込まれている権利および条件を構文解析し、

電子透かし記述を検索し、後の行為の準備を行う。

[0035] 本発明に係る第1のコンテンツ配信方法は、コンテンツに対して、そのコンテンツの著作権を保護するための保護処理を行う第1の保護処理ステップと、前記のコンテンツの利用条件を決定する決定ステップと、前記のコンテンツ若しくは前記のコンテンツのアドレスを有する第1のデジタルアイテムであって、他のデジタルアイテムを内部に定義することが可能なデジタルアイテム、又は前記の第1のデジタルアイテムを内部に定義した第2のデジタルアイテムをデジタルアイテム宣言形式で記述する第1の記述ステップと、デジタルアイテム宣言形式で記述された前記の第1のデジタルアイテム又は第2のデジタルアイテムをパッケージ化するパッケージ化ステップと、パッケージ化された前記の第1のデジタルアイテム又は第2のデジタルアイテムをユーザ端末に配信する配信ステップとを含む。このコンテンツ配信方法は、前記の第1の記述ステップにおいて、前記の第1のデジタルアイテム中に、前記の保護処理に関する記述と前記の利用条件に関する記述が両方記述される。

[0036] 好ましくは、前記のユーザ端末によって前記の利用条件に関する記述が前記の保護処理に関する記述よりも先に解析されるように、前記の第1のデジタルアイテムにおいて、前記の利用条件に関する記述は前記の保護処理に関する記述よりも先に

記述される。

[0037] 好ましくは、前記の第1の記述ステップは、前記の保護処理に関する記述として、前記のコンテンツの著作権が保護されていることを示すフラグと、その保護を解除する保護解除ツールの情報とを記述するステップを含む。この場合のコンテンツ配信方法を第2のコンテンツ配信方法という。

[0038] 好ましくは、前記の第2のコンテンツ配信方法において、前記の第1の保護処理ステップは、前記のコンテンツに電子透かしを埋め込むステップ、前記のコンテンツを暗号化するステップ、及び前記のコンテンツをデジタル署名するステップの少なくとも1つのステップを含み、前記の第1の記述ステップは、前記の保護処理に関する記述として、前記の保護処理の種類に応じて、前記のコンテンツに電子透かしが埋め込まれていることを示すフラグと前記の電子透かしを検出する検出ツールの情報、前記のコンテンツが暗号化されていることを示すフラグと前記のコンテンツを復号化する復号化ツールの情報、及び前記のコンテンツがデジタル署名されていることを示すフラグと前記のデジタル署名を照合する照合ツールの情報の少なくとも1つを記述するステップを含む。この場合のコンテンツ配信方法を第3のコンテンツ配信方法という。

[0039] 好ましくは、前記の第3のコンテンツ配信方法において、前記の第1の保護処理ステップは、暗号鍵を用いて前記のコンテンツを暗号化するステップを含み、前記の第1の記述ステップは、前記の保護処理に関する記述として、前記のコンテンツが暗号化されていることを示すフラグ、前記の復号化ツールの情報、及び前記のコンテンツを暗号化した暗号鍵の情報を記述するステップを含む。この場合のコンテンツ配信方法を第4のコンテンツ配信方法という。

[0040] 好ましくは、前記の第4のコンテンツ配信方法において、前記の第1の保護処理ステップは、暗号鍵をさらに暗号化するステップを含み、前記の第1の記述ステップは、前記の保護処理に関する記述として、さらに、暗号化された前記の暗号鍵を復号するライセンス鍵の情報を記述するステップを含む。この場合のコンテンツ配信方法を第5のコンテンツ配信方法という。

[0041] 好ましくは、前記の第1ー第5の各コンテンツ配信方法は、前記の利用条件に関する記述に対して、その記述の著作権を保護するための保護処理を行う第2の保護処

理ステップと、前記の保護処理に関する記述として、前記の利用条件に関する記述の著作権が保護されていることを示すフラグと、その保護を解除する保護解除ツールの情報とを記述する第2の記述ステップとを含む。

[0042] 本発明に係る第1のコンテンツサーバは、コンテンツに対して、そのコンテンツの著作権を保護するための保護処理を行う保護処理部と、前記のコンテンツの利用条件を生成する利用条件生成部と、前記のコンテンツ若しくは前記のコンテンツのアドレスを有する第1のデジタルアイテムであって、他のデジタルアイテムを内部に定義することが可能なデジタルアイテム、又は前記の第1のデジタルアイテムを内部に定義した第2のデジタルアイテムをデジタルアイテム宣言形式で記述する記述部と、デジタルアイテム宣言形式で記述された前記の第1のデジタルアイテム又は第2のデジタルアイテムをパッケージ化するパッケージング部と、パッケージ化された前記の第1のデジタルアイテム又は第2のデジタルアイテムをユーザ端末に配信する配信部とを含む。このコンテンツサーバにおいて、前記の記述部は、前記の第1のデジタルアイテム中に、前記の利用条件に関する記述と前記の保護処理に関する記述を両方記述する。

[0043] 好ましくは、前記の第1のコンテンツサーバにおいて、前記の記述部は、前記の保護処理に関する記述として、前記のコンテンツの著作権が保護されていることを示すフラグと、その保護を解除する保護解除ツールの情報とを記述する。この場合のコンテンツサーバを第2のコンテンツサーバという。

[0044] 好ましくは、前記の第1及び第2の各コンテンツサーバにおいて、前記の保護処理部は、前記の利用条件に関する記述に対して、その記述の著作権を保護するための保護処理を行い、前記の記述部は、前記の保護処理に関する記述として、前記の利用条件に関する記述の著作権が保護されていることを示すフラグと、その保護を解除する保護解除ツールの情報とを記述する。

発明の効果

[0045] 本発明によるコンテンツ配信方法及びコンテンツサーバによれば、コンテンツ又はコンテンツのアドレスを有するデジタルアイテム中にそのコンテンツに関するIPMP記述とREL記述を両方記述する。これにより、ユーザ端末は、コンテンツ毎にそのコン

テンツに関連したREL記述及びIPMP記述を解析することができる。よって、ユーザは、そのコンテンツを処理するために必要な保護解除ツールのみを取得することが可能になる。また、デジタルアイテムにおいてREL記述をIPMP記述よりも先に記述すれば、ユーザ端末はIPMP記述よりもREL記述を先に解析するので、REL記述に応じて必要な保護解除ツールのみを取得することが可能になる。その結果、ユーザが効率良く、かつ時間を無駄にすることなく保護解除ツールを取得してコンテンツの再生等を行うことが可能になる。

[0046] 本発明は、権利および条件に関してコンテンツを保護する必要がある場合、特にかかるコンテンツが任意のデータ形態であり、さまざまなネットワークによって送信されることが可能である場合に、特に有用である。

[0047] 本発明は、かかる保護を、コンテンツIDによって、保護されるコンテンツに関連付ける必要がある場合、特にかかる保護情報が、コンテンツIDまたはMPEG−21のDIIを用いて保護されるコンテンツに添付される一連の記述として定義される場合に有用である。

[0048] 本発明は、かかる保護が、コンテンツの作成、コンテンツの配布のほか、コンテンツの消費のために明確であり、好都合である一般的なIPMP制御グラフホルダまたはREL−IPMP制御グラフホルダに配置される場合に有用である。かかるホルダは、MPEG−21静的ファイルフォーマットのDIDに保持されてもよく、RTP伝送のためにSDPに保持されてもよい。

[0049] 本発明は、柔軟性、更新可能性および拡張性のために、定義されるIPMPツールおよび外部のIPMPツールの両方を用いることができるように、保護のそれぞれがツールIDによって指示される場合に有用である。

図面の簡単な説明

[0050] [図1]従来技術の包含されている可能な保護情報に関するDID構造を示す図である。

[図2]従来技術のMPEG−21 IPMPアーキテクチャを示す図である。

[図3]本発明の実施の形態1によるコンテンツサーバの構成例を示すブロック図である。

[図4]図3に示されたコンテンツサーバ20によって行われるコンテンツ配信処理を説明するフローチャートの例である。

[図5]個別の権利および保護に関連するコンテンツのパッケージ化のフローチャートである。

[図6]DIDに保持される権利および保護に関する情報のためのIPMP制御グラフである。

[図7]図4に示される記述ステップの詳細を示すフローチャートの他の例を示す。

[図8]図7に示されたフローチャートのステップS45の詳細を示すフローチャートである。

[図9]IPMP制御グラフ情報に関して保護およびパッケージ化されるコンテンツのための端末処理のフローチャートである。

[図10]IPMP制御グラフの処理に関連するIPMPアーキテクチャを示す図である。

[図11]合成した権利および保護に関するコンテンツのパッケージ化のフローチャートである。

[図12]DIDに保持される権利および保護に関する情報のためのIPMP制御グラフである。

[図13]図4に示される記述ステップの詳細を示すフローチャートの他の例を示す。

[図14]REL—IPMP制御グラフ情報に関して保護およびパッケージ化されるコンテンツのための端末処理のフローチャートである。

[図15]REL—IPMP制御グラフの処理に関連するIPMPアーキテクチャを示す図である。

[図16]REL—IPMP制御グラフにおける権利および保護のレイアウトを示す図である。

符号の説明

[0051] 20 コンテンツサーバ

22 入力インタフェース部

23 コンテンツID割り当て部

24 コンテンツ保護処理部

25 利用条件データ生成部

26 DID記述部

27 パッケージング部

28 配信部

5. 1 モジュール

5. 2 モジュール

5. 3 モジュール

5. 4 モジュール

5. 5 モジュール

5. 6 モジュール

5. 7 モジュール

5. 8 モジュール

5. 9 モジュール

5. 10 モジュール

5. 11 モジュール

5. 12 モジュール

5. 13 モジュール

5. 14 モジュール

5. 15 モジュール

発明を実施するための最良の形態

[0052] 図5に示されているようにコンテンツ保護側では、MPEG−21が使用可能であれば、コンテンツ識別子(CID)またはDIIによって識別されるコンテンツに直接関連する権利および保護の情報をすべて包含するために、図7に示されているように、IPMP制御グラフが生成される。

[0053] コンテンツは、指紋、持続的な関連性または、CIDまたは他の情報を埋め込むことによる著作権保護などの一定の機能を実現するために、一定の電子透かしツールを用いて電子透かしを実現することも可能である。

[0054] ツールIDXXXを有するIPMPツールによってコンテンツを暗号化することができる

。尚、xxxは、どの暗号化アルゴリズムが用いられているかを示すために、RA(登録機関)によって登録されている番号である。AESなどのデフォルトツールは、実装される簡素なハードウェアのために定義されている。結果として生じる鍵情報は、IPMP制御グラフに、直接、または全体の鍵情報データを発見することが可能な位置を示すことによって保持されてもよい。暗号鍵をさらに暗号化することができ、最終的にIPMP制御グラフ、RELデータまたは他の権利表現データ、若しくはDID自体、または鍵位置インジケータによってIPMP制御グラフ／REL／DIDに保持されることが指示されうる任意の場所のいずれかにおいてライセンスを生成または直接保持することも可能である。

[0055] しかし、保護されるコンテンツが同期のためにネットワークを介して伝送されるときには、関連するコンテンツのセグメントと共に、鍵情報のセグメントもパッケージ化することが可能であると思われる。

[0056] MPEG−21において定義されるRELなどの独立した既存の技術標準または他の権利表現方法によって、権利を表現することができ、その完全性のためにデジタル署名によってかかる権利を保護することが可能である。

[0057] 図9に示されているようなコンテンツ消費側では、権利および保護情報と共にパッケージ化されるコンテンツは、IPMP制御グラフの構文解析を受け、その結果からコンテンツが保護されているかを知ることができ、さらに、コンテンツが暗号化されているか、電子透かしが入っているか、または権利も保護されているかどうかを決定する。

[0058] 対応する保護ツールが呼び出され、保護されるオブジェクトで動作する。ツールは、MPEG−21標準によって定義され、装置にインストールされる基準となるツールであってもよく、またはツールは著作権を有し、遠隔位置からダウンロードすることができるツールIDによって識別されてもよい。

[0059] ツールは、登録されているツールIDによって識別され、対応するツールを作成するか、または予めツールを配置するように端末または装置に知らせるフラグである。

[0060] 鍵情報は、定義され、IPMP制御グラフに直接的または間接的に保持される鍵データホルダから検索される。鍵情報はまた、コンテンツがネットワークを通じて配布される場合には、保護対象の対応するコンテンツのセグメントと共にセグメントにおいて

入手することも可能である。

[0061] ライセンスマネジャからライセンス情報を入手することができる。ライセンスマネジャは、ライセンスがどのようにライセンスマネジャから検索されるかを一切暴露しないようにするために、耐タンパ性のエンティティであってもよい。

[0062] 権利およびコンテンツは、上記の鍵、鍵データおよび保護ツールを用いることによって、保護されていない状態にされる。権利および条件の処理を行うことができるように、明確な形で、権利および条件を入手するために、権利は権利パーサによってさらに構文解析される。

[0063] したがって、ユーザに付与された権利がある場合には、保護されていないコンテンツの再生、レンダリング、修正、消去または適応を行うことができる。

[0064] 従来技術(非特許文献1および非特許文献2を参照)に関して図1に示されているように、デジタルコンテンツは、関連する可能な保護を有するようにDIDによってパッケージ化される。

[0065] DIDは、定義されているデジタルアイテムのために、「コンテナ」、「アイテム」、「構成要素」、「アンカ」、「記述子」、「条件」、「選択」、「選抜」、「注釈」、「主張」、「リソース」、「断片」、「命令文」(たとえば、図1のユニット1．6、1．7、1．8)などの一連の抽象的な項目及び概念によって形成される有用なモデル(図1のユニット1．1)を定義した。

[0066] 図1に示されているモジュール1．2は、このコンテナ内部で保護されることになっているすべてのアイテムに関して用いられる全体のIPMP制御情報である。モジュール1．3、1．4は、保護されるコンテンツに関連する特定の保護情報である。モジュール1．5は、コンテンツIDを指定するためのDIIである。

[0067] 従来技術に関するさらなる改良点は、DIDが各要素間の静的関係を対処することであり、ファイルフォーマットとして扱われることができるため、権利および保護情報を図5に示されたIPMP__制御__グラフとしてその保護されたコンテンツに直接関連付けることができることである。

[0068] 他方、鍵情報は、IPMP__制御__グラフに直接的または間接的に鍵データホルダから伝送することができる。また、コンテンツがネットワークを通じて配布される場合に

は、鍵情報はセグメント化されてもよい。

[0069] 暗号化も可能である権利は、保護情報とは別に、または保護情報と共に保持される。

[0070] 別の従来技術は、MPEG−21 IPMPアーキテクチャに関して、図2(非特許文献3参照)に示されている。

[0071] モジュール2．1の権利表現言語(REL)エンジンは、認証要求および一連のライセンスおよびルート権限付与が与えられると、REL認証を決定する構成要素である。RELエンジンは、ライセンスマネジャを用いて、認証照会を解決するのを助ける。

[0072] モジュール2．2のデジタルアイテムマネジャは、デジタルアイテムの中のデジタルアイテム宣言を構文解析する。デジタルアイテムマネジャはまた、デジタルアイテムが存在する場所にアクセスし、モジュール2．3のデジタルアイテムインスタンスも作成する。デジタルアイテムマネジャは、デジタルアイテム宣言内に組み込まれている任意のライセンスをライセンスマネジャに伝達する。

[0073] モジュール2．3のデジタルアイテムインスタンスは、信頼されるドメインの中のデジタルアイテムを表す。デジタルアイテムインスタンスは、格納位置および可能であればコンテンツ暗号鍵に関する情報などのデジタルアイテムに関する局所的なメタデータを含む。

[0074] モジュール2．4のライセンスマネジャは、ライセンスの持続状態およびその認証または破棄状況を管理することによって、RELエンジンをサポートする。ライセンスマネジャはまた、ライセンスの完全性の立証を担っている。

[0075] モジュール2．5の条件プロセッサは、条件を選択し、条件を評価し、条件を満たし、一旦、条件が満たされると認証された動作の実行を開始する(DIPプロセッサによって権利の行使を行う)。

[0076] モジュール2．6のIPMPユーザセッションマネジャは、(条件エバリュエータによって)デジタルアイテム動作の呼び出しを指揮し、(RELエンジンによって)適正な認証が入手され、(条件エバリュエータによって)条件が評価されたかを最初に確認する。

[0077] モジュール2．7の権利の行使は、権利を行使したという記録、すなわちデジタルアイテム動作の呼び出しの記録である。この記録は、ユーザセッションマネジャによって

維持され、条件の充足を権利の行使と関連付けるために用いられる。

[0078] モジュール2．8のデジタルアイテム処理エンジンは、デジタルアイテム方法（DIM）、モジュール2．9のデジタルアイテム基本動作（DIBO）、モジュール2．10のデジタルアイテム拡張動作（DIXO）を含むデジタルアイテム動作を実行する。DIMはDIMエンジンによって実行され、DIXOはDIXOエンジンによって実行され、DIBOはDIBOライブラリによって実行される。デジタルアイテム処理エンジンは、処理状態情報に関してユーザセッション状態を更新する。

[0079] 図2に関する大きな問題点は、特に、コンテンツが複数のツールによって保護されており、権利も異なるツールを用いて保護されているときに、処理、解釈および伝送の対象である保護情報がないことである。コンテンツがどのように保護されており、どのように処理される必要があるかを知るための明確な説明がない。

[0080] 図2に関する第2の問題点は、MPEG−21 RELで定義された既存のRELエンジンが権利表現のみを処理するために、ライセンスマネジャからのデータの流れがRELエンジンを通るべきではないことにある。ライセンスマネジャからの出力は、図15に示されるIPMPマネジャである必要があるエンティティによって制御されるコンテンツを復号化するために用いられる暗号鍵を含むことが可能である。復号化自体は、IPMPツール、DIPプロセッサ、DIMEまたはDIBOまたはDIXOで行われてもよい。

[0081] 図2に関する第3の問題点は、RELエンジンが処理するそれらのRELデータがどこから来るかを示すデータの流れの指示がないことである。MPEG−21 RELフォーマットで表現されている場合に権利条件を含むこのような権利表現は、DIDコンテナにおいてDIと共にメタデータとして保持され、DIマネジャによって処理されることが可能である。DIマネジャは、どのDIDが定義されているかに従い、情報を構文解析するだけのDIDパーサに変更すべきである。

[0082] よりよい権利および保護について、2つの事例に基づいて設計される。第1の事例は、対応する権利および条件を表現するために、既存のRELを用いる場合であり、保護制御機構は暗号化、電子透かし、鍵管理を含むコンテンツ保護を考慮して定義される。第2の事例は、暗号化、電子透かし、鍵管理などを含むことが可能な保護機能を追加することによって、既存のRELが拡張される場合である。

[0083] いずれの事例についても以下の節で詳述する。

[0084] 実施の形態1.

(個別の権利および保護を有するコンテンツのパッケージ化および消費)

図3は、本発明の実施の形態1によるコンテンツサーバの構成例を示すブロック図である。図3に示されるように、本実施の形態1によるコンテンツサーバ20は、入力インタフェース部22、コンテンツID割り当て部23、コンテンツ保護処理部24、利用条件データ生成部25、DID記述部26、パッケージング部27、及び配信部28を備える。入力インタフェース部22は、コンテンツサーバ20と外部装置とのインタフェースを行い、このインタフェース部22を介して外部装置からデジタルコンテンツが入力される。コンテンツID割り当て部23は、入力されたコンテンツに対してこのコンテンツを特定するコンテンツIDを割り当てる。コンテンツ保護処理部24は、コンテンツIDが割り当てられたコンテンツに対して、例えば暗号化や電子透かしの埋め込み等の、そのコンテンツの著作権を保護するための保護処理を行う。この保護処理は、保護処理の種類に応じた保護処理ツールを用いて行われる。コンテンツ保護処理部24は、その保護処理ツール及びその保護処理ツールと対となる保護解除ツールに対してツールIDを割り当て、配信部28を介してその保護解除ツールを外部の装置に出力する。ユーザは、必要なときに必要な保護解除ツールを、その外部の装置からダウンロードする。なお、上述したように、保護処理ツールと保護解除ツールとは対になっているので、保護処理ツールのツールIDから保護解除ツールを知ることは可能である。利用条件データ生成部25は、デジタルコンテンツの利用条件を示すデータを生成する。この利用条件のデータは、コンテンツの配信者によって外部の入力装置(図示せず)から直接利用条件データ生成部25に入力されてもよい。

[0085] DID記述部26は、IDが割り当てられたコンテンツ又はそのコンテンツのアドレスを有するデジタルアイテムをデジタルアイテム宣言形式で記述する。また、DID記述部26は、利用条件データ生成部25から入力された利用条件データが示すコンテンツの利用条件に関する記述、及びそのコンテンツに対して行われた保護処理に関する記述をデジタルアイテム中に記述する。パッケージング部27は、デジタルアイテム宣言形式で記述されたデジタルアイテムをパッケージ化する。配信部28は、パッケージ

化されたデジタルアイテムをユーザ端末に配信する。また、配信部28は、コンテンツ保護処理部24から出力された保護解除ツールを外部に出力する。デジタルアイテムは再帰的に定義可能、すなわち自分自身の中に別のデジタルアイテムを定義することが可能である。DID記述部26は、上記コンテンツ又はコンテンツのアドレスを有するデジタルアイテムと同一のデジタルアイテム中に、そのコンテンツの利用条件に関する記述とそのコンテンツの保護処理に関する記述を記述する。

[0086] 図4は、図3に示されたコンテンツサーバ20によって行われるコンテンツ配信処理を説明するフローチャートの例である。図4に示されるように、コンテンツサーバ20は、コンテンツID割り当て部23によって、入力されたコンテンツにIDを割り当て(ステップS1)、コンテンツ保護処理部24によって、そのコンテンツに対して、コンテンツの著作権を保護するための保護処理を行うとともに、その保護を解除する保護解除ツールにIDを割り当てる(ステップS2)。そして、配信部28によって、その保護解除ツールを外部の装置に出力する(ステップS3)。次に、コンテンツサーバ20は、利用条件データ生成部25を用いてそのコンテンツの利用条件を決定する(ステップS4)。次に、コンテンツサーバ20は、DID記述部26によって、そのコンテンツ若しくはコンテンツのアドレスを有するデジタルアイテムをデジタルアイテム宣言形式で記述する(ステップS5)。その際に、デジタルアイテム中に、上記保護解除ツールのID等の保護解除ツールの情報、及び上記利用条件が記述される。次に、コンテンツサーバ20は、パッケージング部27によって、そのデジタルアイテム宣言形式で記述されたデジタルアイテムをパッケージ化する(ステップS6)。最後に、コンテンツサーバ20は、配信部28によって、そのパッケージ化されたデジタルアイテムをコンテンツのユーザ端末に配信する(ステップS7)。

[0087] 図5において、権利および保護スキームに関してコンテンツのパッケージ側が示されている。モジュール5．8のRELは、条件に関係する権利をパッケージ化するために用いられることになっている既存の権利表現言語である。他の部分5．3、5．4、5．5、5．6、5．7、5．9、5．11、5．13は、保護関連機能である。最も重要な部分は、IPMP制御グラフであるモジュール5．15にある。MPEG−21のDIDコンテナに保持されてもよいが、異なるアプリケーションドメインの他の場所に保持されてもよい。

[0088] コンテンツはネットワークによって伝送される必要がある場合に、通常はセグメント化および暗号化が行われ、リソースとしていずれかの場所に格納され、対応する時間変化の鍵が、モジュール5．9においてIPMP制御グラフの鍵データホルダに鍵情報として、直接的または位置を示すことによって間接的に格納される。

[0089] たとえば、保護されるコンテンツがRTPによって伝送されるとき、IPMP制御グラフはSDP（セクション記述プロトコル）に保持され、鍵情報はRTPヘッダに保持されてもよく、または映像および音声パケットのための特殊な事例として、同期化される限り、時間変化の鍵および保護される映像または音声データの中に保持されてもよい。

[0090] モジュール5．1は、コンテンツIDを割り当てることになっており、ここでは、MPEG－21のDIIを用いることが可能である。必要に応じて、サブコンテンツIDを用いることができ、サブコンテンツを保護する必要がある場合には、保護がこのサブコンテンツIDに関連付けられることができる。コンテンツIDの割り当ては、コンテンツ割り当て部23が行う。

[0091] モジュール5．2は、コンテンツが保護されているかフリーであるかを知らせるために、IPMP制御グラフにフラグを配置することになっている。モジュール5．3は、電子透かしが組み込まれているかどうかを示すために、IPMP制御グラフにフラグを配置することになっている。これらのフラグの配置は、DID記述部26によって行われる。

[0092] コンテンツに埋め込まれた電子透かしがある場合には、モジュール5．4は、この事例に用いられるWMツール用に電子透かし（WM）ツールIDを割り当てた後、ツールIDが記録され、IPMP制御グラフに配置される。モジュール5．5は、IPMP制御グラフに配置される電子透かしインタフェースまたはAPI関連情報を含むWM記述を作成する。WMツールIDの割り当ては、コンテンツ保護処理部24によって行われる。また、そのWMツールIDのIPMP制御グラフへの配置、及び上記WM記述の作成は、DID記述部26によって行われる。

[0093] モジュール5．6は、コンテンツが暗号化されているかどうかを決定することになっており、モジュール5．15において「はい／いいえ」に関するフラグがIPMP制御グラフに配置される。このフラグの配置は、DID記述部26によって行われる。

[0094] モジュール5．9は、この事例に用いられる暗号化ツール用に暗号化ツールIDを割

り当て後、ツールIDが記録され、IPMP制御グラフに配置される。モジュール5．7は、IPMP制御グラフに直接、またはホルダによって他の位置を示すことによって鍵データホルダの鍵情報を配置することになっている。暗号化ツールIDの割り当ては、コンテンツ保護処理部24によって行われる。また、その暗号化ツールIDのIPMP制御グラフへの配置、及び上記鍵情報の配置は、DID記述部26によって行われる。

[0095] モジュール5．11、5．13において、暗号鍵がさらに暗号化され、ライセンスとしての鍵がIPMP制御グラフ、REL、DIDまたは鍵位置1によって示される任意の場所に最終的に配置される。暗号鍵の暗号化は、コンテンツ保護処理部24によって行われ、ライセンスとしての鍵の配置は、DID記述部26によって行われる。

[0096] モジュール5．8は、既存のREL標準に適合する対応する条件に関して権利を作成してパッケージ化することになっており、この部分は、コンテンツ配信バリューチェーンの販売代理人によって修正および編集されてもよい。上記権利の作成は、利用条件データ生成部25によって行われる。

[0097] モジュール5．10は、権利をデジタル署名することによって権利のメタデータを保護することになっている。モジュール5．12は、デジタル署名の照合のためのツールIDを割り当てることになっており、モジュール5．14は、IPMP制御グラフ若しくはDID、または鍵位置2によって示される任意の場所にエンティティ__鍵を配置することになっている。権利のデジタル署名、及びデジタル署名の照合のためのツールIDの割り当ては、コンテンツ保護処理部24によって行われる。また、エンティティ__鍵の配置は、DID記述部26によって行われる。

[0098] モジュール5．15の詳細は、XMLに基づくアプローチがIPMP制御グラフを表現するために用いられるMPEG−21の事例における例として図7Aに示されている。DI（DID6．1によって宣言される6．2）は、2つのデジタルアイテム（6．3、6．4）からなり、それぞれのデジタルアイテムは個別の添付されるメディアリソース（6．9、6．10）を有する識別スキーム（6．5、6．6）を有する。モジュール6．7は、上述のIPMP制御グラフを示し、モジュール6．8は、リソースに連係される実際の権利表現（条件および利用規則）を与える。

[0099] 以下に、図6について詳細に説明する。図6は、DID形式で記述されたデジタルア

イテムの一例を示す図である。デジタルアイテムは、再帰的に定義可能、すなわち自分自身の中にデジタルアイテムを有することが可能である。図6に示されるデジタルアイテム6．2は、デジタルアイテム(6．3、6．4)を含む。デジタルアイテム(6．3、6．4)のリソース(6．9，6．10)は、デジタルコンテンツ又はデジタルコンテンツを所有する所有元のアドレスを含む。また、命令文(6．5、6．6)は、それぞれコンテンツIDを指定するためのDIIである。なお、図6に示されたコンテンツ又はコンテンツのアドレスを有するデジタルアイテム(6．3、6．4)は、第1のデジタルアイテムをなし、複数の第1のデジタルアイテムが内部に定義されたデジタルアイテム6．2は、第2のデジタルアイテムをなす。

[0100] 図6に示されるように、コンテンツ又はコンテンツのアドレスを有するデジタルアイテム(6．4)には、そのコンテンツに関するIPMP記述(6．7)とREL記述(6．8)とが両方記述される。表1は、IPMP記述(6．7)の意味を示す。表1において、左欄には実際の記述が示され、右欄には、その記述の簡単な意味が示される。

[表1]

<Watermarking flag = "true">	電子透かし（Watermarking）が埋め込まれている
<Tool ID> 11 </Tool ID>	電子透かしを検出するツールは、ツールＩＤが「１１」のツールである
<WMInfo> <API> OPIMA </API> </WMUInfo>	電子透かしに書き込まれた情報についてのＡＰＩ（パラメータの並び方のフォーマット）は、「ＯＰＩＭＡ」である。
<Encryption flag = "true">	コンテンツは暗号化されている
<Tool ID> 12 </Tool ID>	暗号を復号化するツールは、ツールＩＤが「１２」のツールである
<Name> Default:AES </Name>	復号化ツールの名前は、「Default:AES」である
<KeyData> KeyInformation </KeyData>	暗号鍵の情報の名前は、「KeyInformation」である
<LicenseKey>URI:xxx</LicenseKey>	ライセンス鍵は、特定の場所（URI:xxx）に配置されている

[0101] 表1に示されるように、IPMP記述中の「KeyInformation」は、コンテンツを暗号化

した暗号鍵の鍵情報である。その暗号鍵は、ユーザに配信されるとき、他者に悪用されないように暗号化されている。ライセンス鍵は、この暗号を解くための鍵である。上述のIPMP記述には、そのライセンス鍵が配置された場所が記述されている。

[0102] 次に、表2は、REL記述(6．8)の意味を示す。表2において、左欄には実際の記述が示され、右欄には、その記述の簡単な意味が示される。

[表2]

<grant> <mx:play/> <validityInterval><notBefore> 2001-12-24T23:59:59</notBefore> <notAfter>2002-01-24T23:59:59 </notAfter></validityInterval> </grant>	コンテンツの再生は、２００１年１２月２４日の２３時５９分５９秒から２００２年１月２４日の２３時５９分５９秒までの期間だけ許可されている。
<issuer> <details><timeOfIssue>2001-01-27T 15:30:00</timeOfIssue></details> </issuer>	権利の発行日は、２００１年１月２７日の１５時３０分である。

[0103] 図6に示されるように、コンテンツ又はコンテンツのアドレスを有するデジタルアイテム中にそのコンテンツに関するIPMP記述とREL記述とが両方記述されるので、ユーザ端末は、そのコンテンツに関連したREL記述及びIPMP記述のみを解析すればよく、ユーザ端末は、そのコンテンツを処理するために必要な保護解除ツールのみを取得することができる。

[0104] 図6に示されるように、デジタルアイテム中で、IPMP記述がREL記述よりも先に記述されている場合、ユーザ端末は、IPMP記述を先に解析する。この場合、ユーザ端末は、REL記述の内容によらず、保護解除ツールのダウンロードを行う。例えば、図6に示されたデジタルアイテムを受信した場合、ユーザ端末は、許可されたコンテンツの利用期間が始まる前に必要なツールのダウンロードとセットアップが行う。この場合、ユーザ端末がその利用期間が始まった後にコンテンツの再生を行うときは、保護解除ツールのダウンロードが不要となり、速やかなコンテンツの再生が可能になる。

[0105] なお、図7は、図6に示されるデジタルアイテムを作成する場合の記述ステップ(図4において、ステップS5で示される。)の詳細を示すフローチャートの他の例を示す。

図7に説明されるように、コンテンツサーバ20のDID記述部26は、コンテンツID割り当て部23から入力されたIDのデータを用いて、デジタルアイテムに割り当てられたコンテンツIDを記述する(ステップS41)。そして、コンテンツ保護処理部24から入力されたデータを用いて、コンテンツに電子透かしが埋め込まれているかどうかを判断し(ステップS42)、電子透かしが埋め込まれていると判断するなら(ステップS42でYES)、IPMP記述として、電子透かしが埋め込まれていることを示すフラグ、及び検出ツールの情報、例えば、検出ツールのツールIDを記述する(ステップS43)。埋め込まれていないと判断するなら(ステップS42でNO)、次のステップS44に進む。次に、DID記述部26は、コンテンツ保護処理部24から入力されたデータを用いて、コンテンツが暗号化されているかどうかを判断し(ステップS44)、暗号化されていると判断するなら(ステップS44でYES)、IPMP記述として、暗号化されていることを示すフラグ等を記述する(ステップS45)。暗号化されていないと判断するなら(ステップS44でNO)、次のステップS46に進む。次に、DID記述部26は、コンテンツ保護処理部24から入力されたデータを用いて、コンテンツがデジタル署名されているかどうかを判断し(ステップS46)、デジタル署名されていると判断するなら(ステップS46でYES)、IPMP記述として、電子署名されていることを示すフラグ、及び照合ツールの情報、例えば、照合ツールのツールIDを記述する(ステップS47)。デジタル署名されていないと判断するなら(ステップS46でNO)、次のステップS48に進む。最後に、DID記述部26は、利用条件データ生成部25から入力されたデータを用いて、REL記述として、コンテンツの利用条件を記述する(ステップS48)。

[0106] 図8は、図7に示されたフローチャートのステップS45の詳細を示すフローチャートである。DID記述部26は、コンテンツが暗号化されているなら(ステップS44でYES)、IPMP記述として、コンテンツが暗号化されていることを示すフラグ、復号化ツールID等の復号化ツールの情報、及び暗号鍵の情報を記述する(ステップS452)。そして、再度コンテンツ保護処理部24から入力されたデータを用いて、暗号鍵がさらに暗号化されているかどうかを判断し(ステップS452)、暗号化されていると判断するなら(ステップS452でYES)、IPMP記述として、暗号鍵を復号するライセンス鍵の情報を記述する(ステップS453)。暗号化されていないと判断するなら(ステップS452

でNO)、図7に示されるステップS46に進む。

[0107] なお、REL記述(権利のメタデータ)に対して保護処理が行われてもよい。その場合、DID記述部26は、利用条件データ生成部25から入力されたデータを用いて、REL記述を作成し、そのREL記述をコンテンツ保護処理部24に入力する。コンテンツ保護処理部24は、入力されたREL記述に対して保護処理を行う。このとき、コンテンツサーバ20が行う処理は、コンテンツに対して保護処理が行われた場合の処理と同様である。具体的には、図4のステップS2, S3に示される処理が行われる。その後、DID記述部26は、コンテンツ保護処理部24から入力されたデータを用いて、上記保護処理の種類に応じたフラグ、及び保護解除ツールの情報をデジタルアイテムに記述する。この記述処理は、コンテンツに対して保護処理が行われた場合にDID記述部26が行う処理と同様である。具体的には、図7に示されたステップS42ーS47の処理が行われる。

[0108] 図9は、保護されるコンテンツをモジュール9.18で消費することが可能になる前に、IPMP制御グラフに保持される保護およびパッケージ化情報を処理するための端末処理のフローチャートを示している。

[0109] モジュール9.1は、IPMP制御グラフがMPEG−21のDIDに保持される場合にのみDIDパーサが必要とされるときに、DIDおよびIPMP制御グラフ情報を構文解析することになっている。

[0110] RTPネットワークによるコンテンツの配信の場合には、鍵情報が時間変化である場合には、鍵情報を除く権利および保護記述情報を入手するために、SDPからIPMP制御グラフを検索することができる。

[0111] モジュール9.2は、コンテンツが保護されているかまたはフリーであるかを検出することになっている。コンテンツがフリーである場合には、消費のためにモジュール9.18によって再生されることができる。そうでない場合には、モジュール9.3、9.4、9.5にそれぞれ進んで確認するための分岐が3つ存在する。

[0112] モジュール9.3は、権利が暗号化されているかどうかを検出することになっており、モジュール9.4は、コンテンツが暗号化されているかを検出することになっており、モジュール9.5はコンテンツに電子透かしが入っているかどうかを検出することになっ

ている。

[0113] 権利が保護されている場合には、モジュール9．6はツールIDを有する保護ツールを呼び出すことになっており、モジュール9．7はツールを用いて権利の完全性を確認することになっている。モジュール9．8において完全性が首尾よく証明される場合には、既存のREL標準に適合するRELエンジンによって権利を構文分析するために、権利がモジュール9．9に送信される。

[0114] モジュール9．11は、コンテンツに添付される権利および条件を処理し、バッファに付与された権利および条件を格納する。モジュール9．19において、ユーザによって要求される権利が、バッファに格納された権利および条件に反していないかどうかの確認がなされる。

[0115] 権利に保持されているライセンスがある場合には、モジュール9．10は、保護される耐タンパ性（TR）であってもよいライセンスマネジャからライセンスを検索することになっている。

[0116] コンテンツが保護および暗号化されている場合には、モジュール9．13は、IPMP制御グラフに保持されているツールIDによって示される暗号化ツールを呼び出すことになっており、モジュール9．14は鍵情報を検索することになっており、モジュール9．12はライセンスマネジャから鍵ライセンスを入手することになっている。

[0117] ここでは、復号化エンジンがコンテンツの保護を外すために用いる実際のライセンスをライセンスマネジャが提供するため、ライセンスマネジャが端末の一部または他の場所の任意の場所であるならば、耐タンパ技術によって保護されてもよい。

[0118] 暗号化ツールは、大部分の端末がその実装に用いるデフォルトとして定義されることが可能であり、特殊なドメインにおけるデフォルトの暗号化ツール以外のものを選択することができるようにIPMPツールIDが提供される。プラットホームはツールIDによって指示される異なる暗号化ツールをダウンロードして用いることが許容される場合には、異なるドメインにわたって相互運用性を実現すると同時に、拡張性、柔軟性および更新可能性を実現することになる。

[0119] さまざまなネットワークによるコンテンツ配信の場合には、異なる場所から鍵情報を検索することができてもよい。これは、鍵情報を配置する場所に左右される。RTPへ

ッダに鍵情報を配置する場合には、RTPヘッダで入手することができ、映像および音声データなどの他のパケットとして配置される場合には、映像および音声に適用されるものと同一の規則に従って入手することができる。映像および音声のコンテンツを復号化する必要がある場合には、時間変化の鍵情報を同時に入手する必要がある。

[0120] モジュール9．15は、呼び出されたツール、鍵データおよびライセンスを有するコンテンツを復号化し、さらなる処理のためにモジュール9．17に伝送されることになっている。

[0121] モジュール9．5において、コンテンツが電子透かし入りであると検出される場合には、モジュール9．16において、ツールIDを有する電子透かしツールおよびインタフェースをはじめとするその記述データが呼び出され、ユーザの要求に合致する行為の準備が施される。

[0122] 最終的に、モジュール9．17は、与えられた権利および条件に基づいて、ユーザが要求する権利を行使し、モジュール9．15の出力である保護されていないコンテンツに作用することになっている。

[0123] 図9において、耐タンパは、保護されていないコンテンツを入手するためのコンテンツの復号化であっても、ライセンス、権利および条件処理を提供して、権利を準備するライセンスマネジャの機能を保護するために用いられる。

[0124] 図10は、個別に処理されるRELおよびIPMP制御グラフを有する修正されたIPMPアーキテクチャを示している。図9および図10の権利および保護（IPMPに関連する）機能を比較すると、図2の従来技術には欠けているIPMPに関連する機能が多くあることが明白である。RELエンジンに関するモジュール9．9、ライセンスマネジャに関するモジュール9．10、9．12、および条件処理に関するモジュール9．11である図9では青色のブロックのみが図2に示されている従来技術に導入されている。このような機能ブロックは、図2ではモジュール2．1、モジュール2．4およびモジュール2．5である。

[0125] 図10に示されているように、モジュール10．11がIPMP制御グラフ情報を構文解析して処理するために加えられ、対応する結果がモジュール10．4のライセンスマネジャに伝達され、RELに関連するデータはその完全性が確認された後、モジュール

10．1のRELエンジンに伝達され、コンテンツ保護および電子透かし情報がさらなる処理のために、モジュール10．3のDIインスタンスに伝達される。

[0126] モジュール10．12の復号化、電子透かしなどは、かかる方法がDIMEで定義されている場合にはモジュール10．8において行われてもよく、またはDIBOの1つの機能として定義されている場合にはモジュール10．9において行われてもよく、または外部の機能である場合にはモジュール10．10において行われてもよい。

[0127] 線10．14はIPMP制御グラフ処理モジュールからRELエンジンへのデータの流れを示しており、線10．15はIPMP制御グラフ処理モジュールからDIインスタンスへのデータの流れを示している。

[0128] 線10．16は、ライセンスを発行するために、ライセンスマネジャからモジュール10．12の保護されていないブロックへのデータの流れを示している。

[0129] モジュール10．13は、図2と比較して同一の信頼されるドメインに配置されるイベント報告エンジンのためである。

[0130] TRは、ライセンスマネジャ動作および条件処理動作を保護するために用いられることになっている耐タンパモジュールを意味する。

[0131] 他のモジュールは、図2に説明されたものと類似の意味である。

[0132] 実施の形態2．

（合成した権利および保護を有するコンテンツのパッケージ化および消費）

本実施の形態2によるコンテンツサーバは、実施の形態1によるコンテンツサーバとその構成及び動作が同一であるので、説明を省略する。

この場合には、権利と保護との明確な境界がなく、権利および保護は混合され、IPMP制御グラフをREL−IPMP制御グラフと考えることができる。

[0133] 現在のMPEG−21 RELまたは他の権利表現言語に基づいて、コンテンツの保護のほか、コンテンツの保護方法の明記が定義されていない。この場合には、既存のRELは、かかる保護信号発信をサポートするために拡張される必要がある。

[0134] 図5に基づく図11に示されているように、モジュール11．16は、既存のREL標準を拡張することによって、コンテンツ保護信号発信をサポートするREL＋拡張とみなされ、モジュール11．15はREL−IPMP制御グラフに変更される。モジュール11．8は

、既存のREL機能である。

[0135] 他のモジュールは、上記で説明したものと同一の機能である。

[0136] 図11に示されているように、権利および保護スキームに関してコンテンツのパッケージ化側を示している。モジュール11．8のRELは、その条件に関連する権利をパッケージ化するために用いられることになっている既存の権利表現言語である。他の部分11．3、11．4、11．5、11．6、11．7、11．9、11．11、11．13は、保護関連機能である。最も重要な部分は、REL−IPMP制御グラフであるモジュール11．15にある。MPEG−21のDIDコンテナに保持されるが、異なるアプリケーションドメインにおいて用いられる場合には他の場所に保持されてもよい。

[0137] コンテンツはネットワークによって伝送される必要がある場合に、通常はセグメント化および暗号化が行われ、リソースとしていずれかの場所に格納され、対応する時間変化の鍵が、モジュール11．9においてREL−IPMP制御グラフの鍵データホルダに鍵情報として、直接的に、または位置を示すことによって間接的に格納される。

[0138] たとえば、保護されるコンテンツがRTPによって伝送されるとき、REL−IPMP制御グラフはSDP(セクション記述プロトコル)に保持され、鍵情報はRTPヘッダに保持されてもよく、または映像および音声パケットのための特殊な事例として、同期化される限り、時間変化の鍵および保護される映像または音声データの中に保持されてもよい。

[0139] モジュール11．1は、コンテンツIDを確認することになっており、ここで、MPEG−21のDIIを用いることが可能である。モジュール11．2は、コンテンツが保護されているかフリーであるかを知らせるために、REL−IPMP制御グラフにフラグを配置することになっている。モジュール11．3は、電子透かしが組み込まれているかどうかを示すために、REL−IPMP制御グラフにフラグを配置することになっている。

[0140] コンテンツに埋め込まれた電子透かしがある場合には、モジュール11．4は、この事例に用いられるWMツール用に電子透かし(WM)ツールIDを割り当てた後、ツールIDが記録され、REL−IPMP制御グラフに配置される。モジュール11．5は、REL−IPMP制御グラフに配置される電子透かしインタフェースまたはAPI関連情報を含むWM記述を作成する。

[0141] モジュール11．6は、コンテンツが暗号化されているかどうかを決定することになっており、モジュール11．15において「はい／いいえ」に関するフラグがREL−IPMP制御グラフに配置される。

[0142] モジュール11．9は、この事例に用いられる暗号化ツール用に暗号化ツールIDを割り当て後、ツールIDが記録され、REL−IPMP制御グラフに配置される。モジュール11．7は、REL−IPMP制御グラフに直接、またはホルダによって他の位置を示すことによって鍵データホルダの鍵情報を配置することになっている。

[0143] モジュール11．11、11．13において、暗号鍵がさらに暗号化され、ライセンスとしての鍵がREL−IPMP制御グラフ、REL、DIDまたは鍵位置1によって示される任意の場所に最終的に配置される。

[0144] モジュール11．8は、既存のREL標準に適合する対応する条件に関して権利を作成してパッケージ化することになっており、この部分は、コンテンツ配信バリューチェーンの販売代理人によって修正および編集されてもよい。

[0145] モジュール11．10は、権利をデジタル署名することによって権利のメタデータを保護することになっている。モジュール11．12は、デジタル署名の照合のためのツールIDを割り当てることになっており、モジュール11．14は、REL−IPMP制御グラフ若しくはDIDまたは鍵位置2によって示される任意の場所にエンティティ__鍵を配置することになっている。

[0146] モジュール11．15の詳細は、XMLに基づくアプローチがREL−IPMP制御グラフを表現するために用いられるMPEG−21の事例において実施例として図12に示されている。図は、図6と類似である。図6に示されているモジュール6．7、6．8の代わりにREL−IPMP制御グラフ（12．11）を用いるが、すべての権利および保護情報を表すために、類似の機能として作用する。

[0147] ここではREL IPMP拡張は権利表現のみならず、保護記述も含むと定義され、権利、条件のほか、原理および発行者を表すためだけに元々は定義されていたことから、かかる拡張は既存のMPEG−21 RELまたは他の権利表現言語に加えて行われることが図12から分かる。図12のXML表現に示されているipmpxは、保護のためのRELの拡張部分である。

[0148] 図12は、DID形式で記述された他のデジタルアイテムの例を示す図である。IPMP記述及びREL記述(12．11)の内容は、図6と同一であるが、図6と異なり、REL記述が最初に記述されている。これは、DID記述部26がIPMP記述よりもREL記述を先に記述することによる。これにより、ユーザ端末は、IPMP記述よりもREL記述を先に解析するので、保護解除ツールをダウンロードする前に、コンテンツの再生が可能かどうか、すなわち再生が許可されている期間かどうかを知ることができる。よって、再生が許可されていない期間の場合は、保護解除ツールをダウンロードする必要がないので、ダウンロードに費やす時間及びコストを省略できる。

[0149] なお、図13は、図12に示されるデジタルアイテムを作成する場合の記述ステップ(図4において、ステップS5で示される。)の詳細を示すフローチャートの他の例を示す。図13に説明されるように、コンテンツサーバ20のDID記述部26は、コンテンツID割り当て部23から入力されたIDのデータを用いて、デジタルアイテムに割り当てられたコンテンツIDを記述する(ステップS51)。そして、利用条件データ生成部25から入力されたデータを用いて、REL記述として、コンテンツの利用条件を記述する(ステップS52)。次に、DID記述部26は、コンテンツ保護処理部24から入力されたデータを用いて、コンテンツに電子透かしが埋め込まれているかどうかを判断し(ステップS53)、電子透かしが埋め込まれていると判断するなら(ステップS53でYES)、IPMP記述として、電子透かしが埋め込まれていることを示すフラグ、及び検出ツールの情報を記述する(ステップS54)。埋め込まれていないと判断するなら(ステップS53でNO)、次のステップS55に進む。次に、DID記述部26は、コンテンツ保護処理部24から入力されたデータを用いて、コンテンツが暗号化されているかどうかを判断し(ステップS55)、暗号化されていると判断するなら(ステップS55でYES)、IPMP記述として、暗号化されていることを示すフラグ等を記述する(ステップS56)。暗号化されていないと判断するなら(ステップS55でNO)、次のステップS57に進む。次に、DID記述部26は、コンテンツ保護処理部24から入力されたデータを用いて、コンテンツがデジタル署名されているかどうかを判断し(ステップS57)、デジタル署名されていると判断するなら(ステップS57でYES)、IPMP記述として、電子署名されていることを示すフラグ、及び照合ツールの情報を記述する(ステップS58)。デジタル署

名されていないと判断するなら(ステップS57でNO)、処理を終了する。なお、図13のステップS56で示された処理は、図8を用いて説明された処理と同一である。

[0150] あるコンテンツに関するIPMP記述とREL記述を、そのコンテンツを有するデジタルアイテム中に両方記述し、それらのIPMP記述とREL記述を同一のパッケージに収めて端末に配信するという本発明の特徴は、例えば、以下のような場合にも応用できる。

[0151] REL記述に、あるコンテンツが複数の解像度で視聴可能であることが記述され、IPMP記述に、各解像度についてそのコンテンツを復号化する際に必要な復号化ツールが全て記述されている場合、1つのコンテンツに関するIPMP記述とREL記述が、別個のデジタルアイテムにそれぞれ記載され、受信側でそれらのREL記述とIPMP記述とを別々に解釈するなら、IPMP記述が解釈された時点で、各解像度で視聴する場合に必要な全ての復号化ツールが一括ダウンロードされる。この場合、ユーザが特定の1つの解像度で視聴することを希望していても、全ての復号化ツールがダウンロードされることになるので、使わない復号化ツールの伝送に多くの時間と費用がかかり、又使わないツールを保存しておくためのメモリも確保しておく必要があるという問題がある。これに対し、IPMP記述とREL記述とを、そのコンテンツを有するデジタルアイテム中に両方記述して、同一のパッケージで配信すると、ユーザが希望する解像度について必要な復号化ツールのみをダウンロードすることが可能となり、復号化ツールの伝送のための時間及びコストを最小にでき、不要なツールをメモリに格納しておく必要もないという効果がある。

[0152] 図9に基づく図14に示されているように、モジュール14．19は、拡張されたRELによってコンテンツ保護もサポートするためにREL＋拡張とみなされ、モジュール14．9は既存のRELエンジンである。モジュール14．1はREL−IPMP制御グラフに変更され、モジュール14．0はMPEG−21の場合には個別のDIDパーサである。

[0153] 他のモジュールは、上記で説明したものと同一の機能である。

[0154] 図14には、保護されるコンテンツがモジュール14．18で消費することが可能になる前に、REL−IPMP制御グラフに保持される保護およびパッケージ化情報を処理するための端末処理のフローチャートが示されている。

[0155] モジュール14．1は、REL−IPMP制御グラフがMPEG−21のDIDに保持される場合にのみDIDパーサが必要とされるときに、DIDおよびREL−IPMP制御グラフ情報を構文解析することになっている。

[0156] RTPネットワークによるコンテンツの配信の場合には、鍵情報が時間変化である場合には、鍵情報を除く権利および保護記述情報を入手するために、SDPからREL−IPMP制御グラフを検索することができる。

[0157] モジュール14．2は、コンテンツが保護されているかまたはフリーであるかを検出することになっている。コンテンツがフリーである場合には、消費のためにモジュール14．18によって再生されることができる。そうでない場合には、モジュール14．3、14．4、14．5にそれぞれ進んで確認するための分岐が3つ存在する。

[0158] モジュール14．3は、権利が暗号化されているかどうかを検出することになっており、モジュール14．4は、コンテンツが暗号化されているかを検出することになっており、モジュール14．5はコンテンツに電子透かしが入っているかどうかを検出することになっている。

[0159] 権利が保護されている場合には、モジュール14．6はツールIDを有する保護ツールを呼び出すことになっており、モジュール14．7はツールを用いて権利の完全性を確認することになっている。モジュール14．8において完全性が首尾よく証明される場合には、既存のREL標準に適合するRELエンジンによって権利を構文分析するために、権利がモジュール14．9に送信される。

[0160] モジュール14．11は、コンテンツに添付される権利および条件を処理し、バッファに付与された権利および条件を格納する。モジュール14．19において、ユーザによって要求される権利が、バッファに格納された権利および条件に反していないかどうかの確認がなされる。

[0161] 権利に保持されているライセンスがある場合には、モジュール14．10は、保護される耐タンパ性(TR)であってもよいライセンスマネジャからライセンスを検索することになっている。

[0162] コンテンツが保護および暗号化されている場合には、モジュール14．13は、REL−IPMP制御グラフに保持されているツールIDによって示される暗号化ツールを呼び

出すことになっており、モジュール14．14は鍵情報を検索することになっており、モジュール14．12はライセンスマネジャから鍵ライセンスを入手することになっている。

[0163] ここでは、復号化エンジンがコンテンツの保護を外すために使用する実際のライセンスをライセンスマネジャが提供するため、ライセンスマネジャが端末の一部または他の場所の任意の場所であるならば、耐タンパ技術によって保護されてもよい。

[0164] 暗号化ツールは、大部分の端末がその実装に用いるデフォルトとして定義されることが可能であり、特殊なドメインにおけるデフォルトの暗号化ツール以外のものを選択することができるようにIPMPツールIDが提供される。プラットホームはツールIDによって指示される異なる暗号化ツールをダウンロードして用いることが許容される場合には、異なるドメインにわたって相互運用性を実現すると同時に、拡張性、柔軟性および更新可能性を実現することになる。

[0165] さまざまなネットワークによるコンテンツ配信の場合には、異なる場所から鍵情報を検索することができてもよい。これは、鍵情報を配置する場所に左右される。RTPヘッダに鍵情報を配置する場合には、RTPヘッダで入手することができ、映像および音声データなどの他のパケットとして配置される場合には、映像および音声に適用されるものと同一の規則に従って入手することができる。映像および音声のコンテンツを復号化する必要がある場合には、時間変化の鍵情報を同時に入手する必要がある。

[0166] モジュール14．15は、呼び出されたツール、鍵データおよびライセンスを有するコンテンツを復号化し、さらなる処理のためにモジュール14．17に伝送されることになっている。

[0167] モジュール14．5において、コンテンツが電子透かし入りであると検出される場合には、モジュール14．16において、ツールIDを有する電子透かしツールおよびインタフェースを含むその記述データが呼び出され、ユーザの要求に合致するまで行為の準備が施される。

[0168] 最終的に、モジュール14．17は、与えられた権利および条件に基づいて、ユーザが要求する権利を行使し、モジュール14．15の出力である保護されていないコンテンツに作用することになっている。

[0169] 図14において、耐タンパは、保護されていないコンテンツを入手するためのコンテ

ンツの復号化であっても、ライセンス、権利および条件処理を提供して、権利を準備するライセンスマネジャの機能を保護するために用いられる。

[0170] 図15は、REL－IPMP制御グラフを有する修正されたIPMPアーキテクチャを示している。図14および図15の権利および保護（IPMPに関連する）機能を比較すると、図2の従来技術には欠けているIPMPに関連する機能が多くあることが明白である。RELエンジンに関するモジュール14．9、ライセンスマネジャに関するモジュール14．10、14．12および条件処理に関するモジュール14．11である図14では青色のブロックのみが図2に示されている従来技術に導入されている。このような機能ブロックは、図2ではモジュール2．1、モジュール2．4およびモジュール2．5である。

[0171] 図15に示されているように、モジュール15．11がIPMP制御グラフ情報を構文解析して処理するために加えられ、対応する結果がモジュール15．4のライセンスマネジャに伝達され、RELに関連するデータはその完全性が確認された後、モジュール15．1のRELエンジンに伝達され、コンテンツ保護および電子透かし情報がさらなる処理のために、モジュール15．3のDIインスタンスに伝達される。

[0172] モジュール15．12の復号化、電子透かしなどは、かかる方法がDIMEで定義されている場合にはモジュール15．8において行われてもよく、またはDIBOの1つの機能として定義されている場合にはモジュール15．9において行われてもよく、または外部の機能である場合にはモジュール15．10において行われてもよい。

[0173] 線15．14はREL－IPMP制御グラフ処理モジュールからRELエンジンへのデータの流れを示しており、線15．15はREL－IPMP制御グラフ処理モジュールからDIインスタンスへのデータの流れを示している。

[0174] 線15．16は、ライセンスを発行するために、ライセンスマネジャからモジュール15．12の保護されていないブロックへのデータの流れを示している。

[0175] モジュール15．13は、図2と比較して同一の信頼されるドメインに配置されるイベント報告エンジンのためである。

[0176] TRは、ライセンスマネジャ動作および条件処理動作を保護するために用いられることになっている耐タンパモジュールを意味する。

[0177] 他のモジュールは、図2に説明したものと類似の意味である。

[0178] 図16には、IPMP制御グラフまたはREL−IPMP制御グラフにおける権利および保護のレイアウトが示されており、コンテンツID、保護されるオブジェクトのインジケータ、保護フラグ、詳細な権利および条件のほか、詳細な保護記述がこのホルダに配置および保持されている。

[0179] 本発明は特定の実施の形態について説明されてきたが、当業者にとっては他の多くの変形例、修正、他の利用が明らかである。よって、本発明は、ここでの特定の開示に限定されず、添付の請求の範囲によってのみ限定され得る。

請求の範囲

[1] コンテンツに対して、そのコンテンツの著作権を保護するための保護処理を行う第1の保護処理ステップと、

前記コンテンツの利用条件を決定する決定ステップと、

前記コンテンツ若しくは前記コンテンツのアドレスを有する第1のデジタルアイテムであって、他のデジタルアイテムを内部に定義することが可能なデジタルアイテム、又は前記第1のデジタルアイテムを内部に定義した第2のデジタルアイテムをデジタルアイテム宣言形式で記述する第1の記述ステップと、

デジタルアイテム宣言形式で記述された前記第1のデジタルアイテム又は第2のデジタルアイテムをパッケージ化するパッケージ化ステップと、

パッケージ化された前記第1のデジタルアイテム又は第2のデジタルアイテムをユーザ端末に配信する配信ステップと

を含むコンテンツ配信方法であって、

前記第1の記述ステップにおいて、前記第1のデジタルアイテム中に、前記保護処理に関する記述と前記利用条件に関する記述が両方記述されることを特徴とするコンテンツ配信方法。

[2] 前記ユーザ端末によって前記利用条件に関する記述が前記保護処理に関する記述よりも先に解析されるように、前記第1のデジタルアイテムにおいて、前記利用条件に関する記述は前記保護処理に関する記述よりも先に記述されることを特徴とする請求項1に記載のコンテンツ配信方法。

[3] 前記第1の記述ステップは、前記保護処理に関する記述として、前記コンテンツの著作権が保護されていることを示すフラグと、その保護を解除する保護解除ツールの情報とを記述するステップを含むことを特徴とする請求項1又は2に記載のコンテンツ配信方法。

[4] 前記第1の保護処理ステップは、前記コンテンツに電子透かしを埋め込むステップ、前記コンテンツを暗号化するステップ、及び前記コンテンツをデジタル署名するステップの少なくとも1つのステップを含み、

前記第1の記述ステップは、前記保護処理に関する記述として、前記保護処理の

種類に応じて、前記コンテンツに電子透かしが埋め込まれていることを示すフラグと前記電子透かしを検出する検出ツールの情報、前記コンテンツが暗号化されていることを示すフラグと前記コンテンツを復号化する復号化ツールの情報、及び前記コンテンツがデジタル署名されていることを示すフラグと前記デジタル署名を照合する照合ツールの情報の少なくとも1つを記述するステップを含むことを特徴とする請求項3に記載のコンテンツ配信方法。

[5] 前記第1の保護処理ステップは、暗号鍵を用いて前記コンテンツを暗号化するステップを含み、

前記第1の記述ステップは、前記保護処理に関する記述として、前記コンテンツが暗号化されていることを示すフラグ、前記復号化ツールの情報、及び前記コンテンツを暗号化した暗号鍵の情報を記述するステップを含むことを特徴とする請求項4に記載のコンテンツ配信方法。

[6] 前記第1の保護処理ステップは、暗号鍵をさらに暗号化するステップを含み、

前記第1の記述ステップは、前記保護処理に関する記述として、さらに、暗号化された前記暗号鍵を復号するライセンス鍵の情報を記述するステップを含むことを特徴とする請求項5に記載のコンテンツ配信方法。

[7] 前記利用条件に関する記述に対して、その記述の著作権を保護するための保護処理を行う第2の保護処理ステップと、

前記保護処理に関する記述として、前記利用条件に関する記述の著作権が保護されていることを示すフラグと、その保護を解除する保護解除ツールの情報とを記述する第2の記述ステップと

を含むことを特徴とする請求項1から6のいずれかに記載のコンテンツ配信方法。

[8] コンテンツに対して、そのコンテンツの著作権を保護するための保護処理を行う保護処理部と、

前記コンテンツの利用条件を生成する利用条件生成部と、

前記コンテンツ若しくは前記コンテンツのアドレスを有する第1のデジタルアイテムであって、他のデジタルアイテムを内部に定義することが可能なデジタルアイテム、又は前記第1のデジタルアイテムを内部に定義した第2のデジタルアイテムをデジタル

アイテム宣言形式で記述する記述部と、

デジタルアイテム宣言形式で記述された前記第1のデジタルアイテム又は第2のデジタルアイテムをパッケージ化するパッケージング部と、

パッケージ化された前記第1のデジタルアイテム又は第2のデジタルアイテムをユーザ端末に配信する配信部と

を含むコンテンツサーバであって、

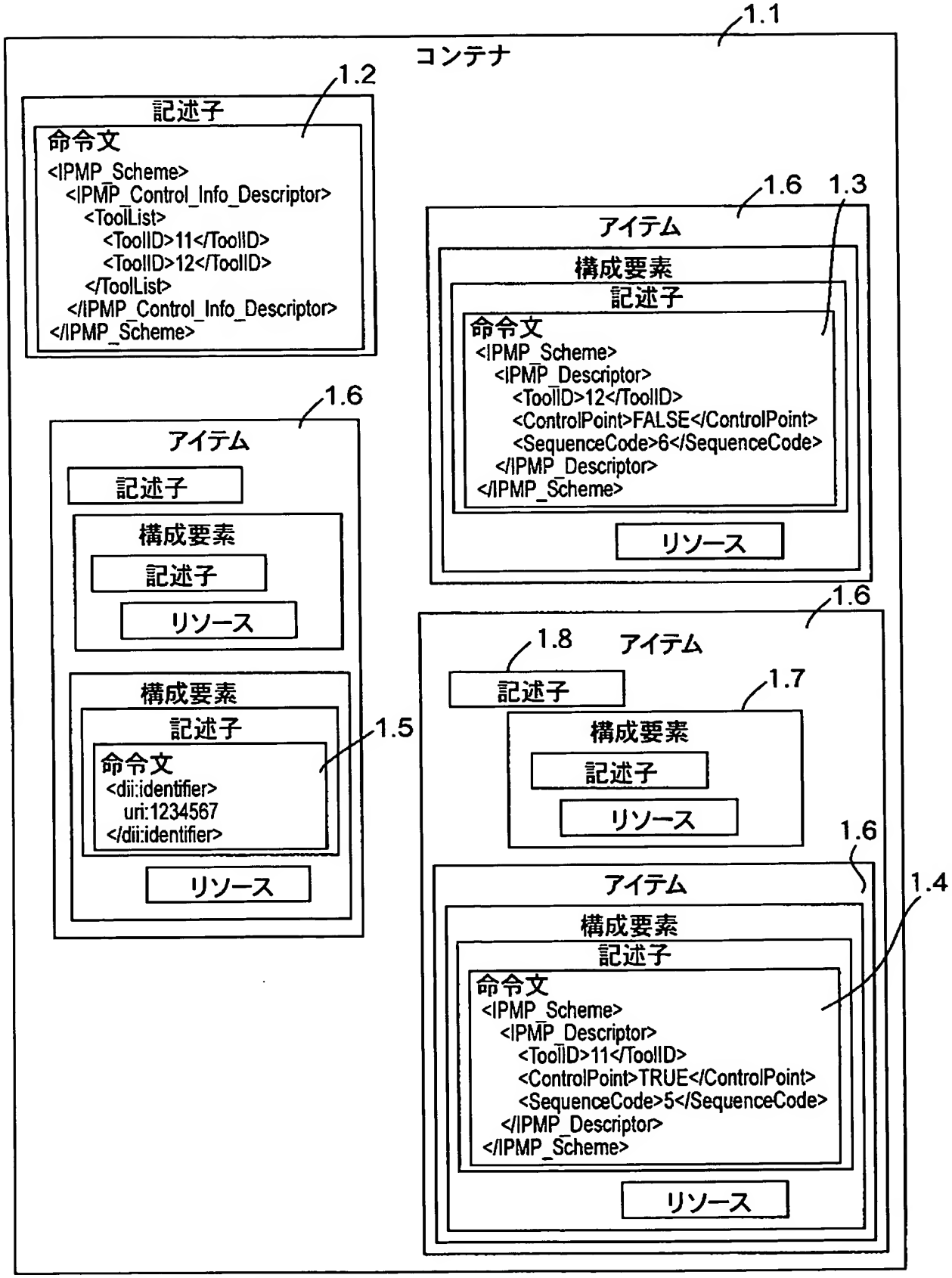
前記記述部は、前記第1のデジタルアイテム中に、前記利用条件に関する記述と前記保護処理に関する記述を両方記述することを特徴とするコンテンツサーバ。

[9] 前記記述部は、前記保護処理に関する記述として、前記コンテンツの著作権が保護されていることを示すフラグと、その保護を解除する保護解除ツールの情報とを記述することを特徴とする請求項8に記載のコンテンツサーバ。

[10] 前記保護処理部は、前記利用条件に関する記述に対して、その記述の著作権を保護するための保護処理を行い、

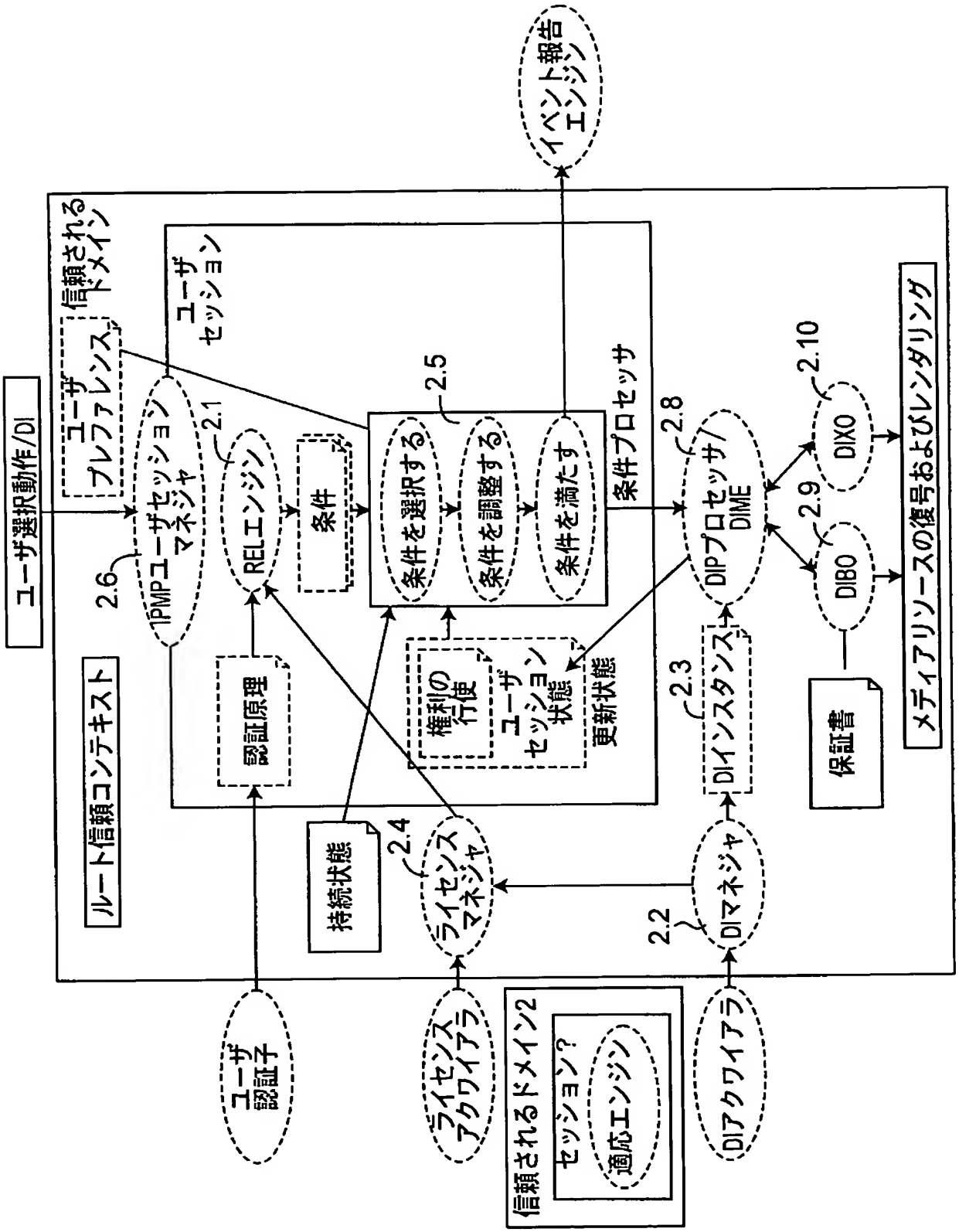
前記記述部は、前記保護処理に関する記述として、前記利用条件に関する記述の著作権が保護されていることを示すフラグと、その保護を解除する保護解除ツールの情報とを記述することを特徴とする請求項8又は9に記載のコンテンツサーバ。

[図1]

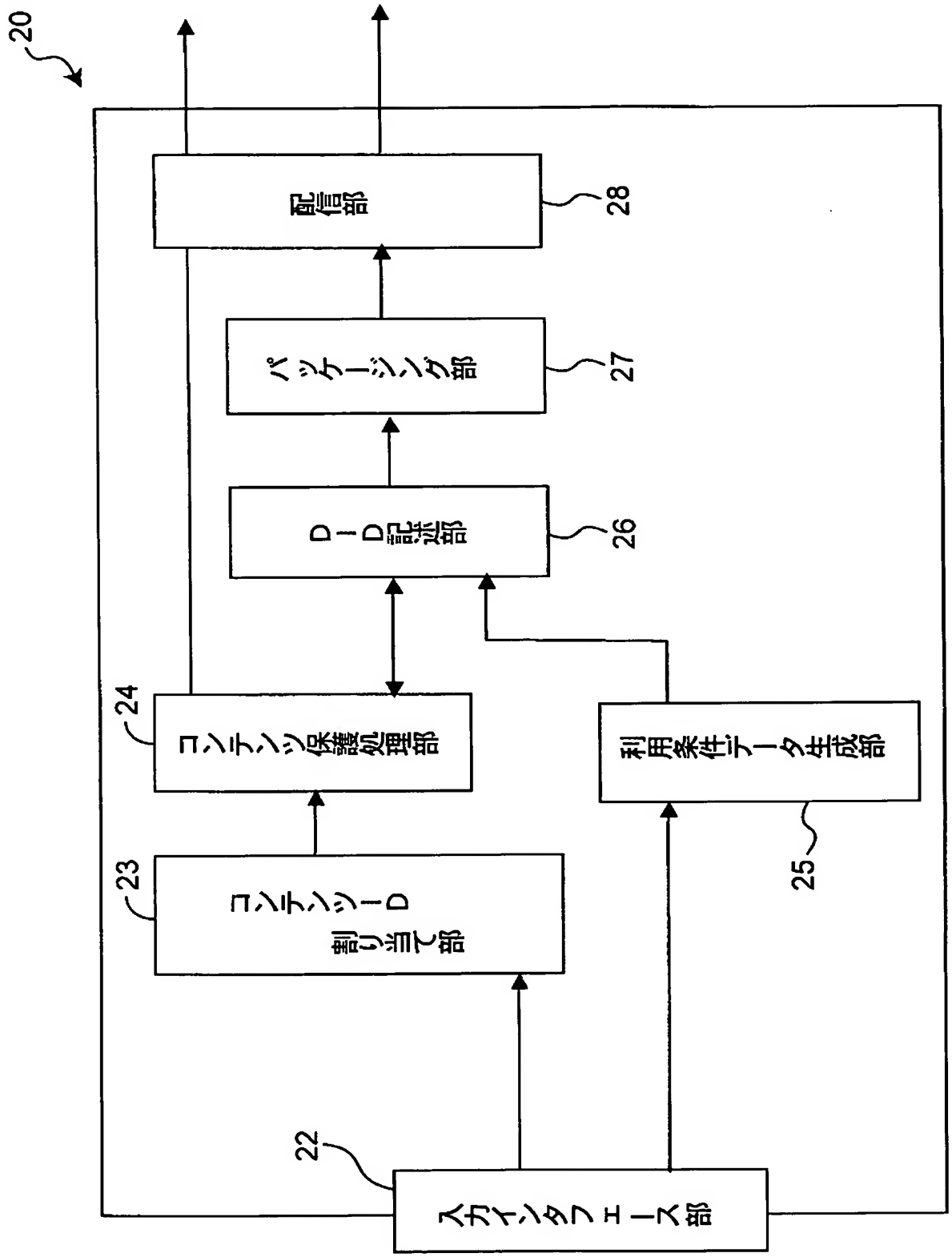


ディジタルアイテム識別(DII)　　IPMP_スキーム

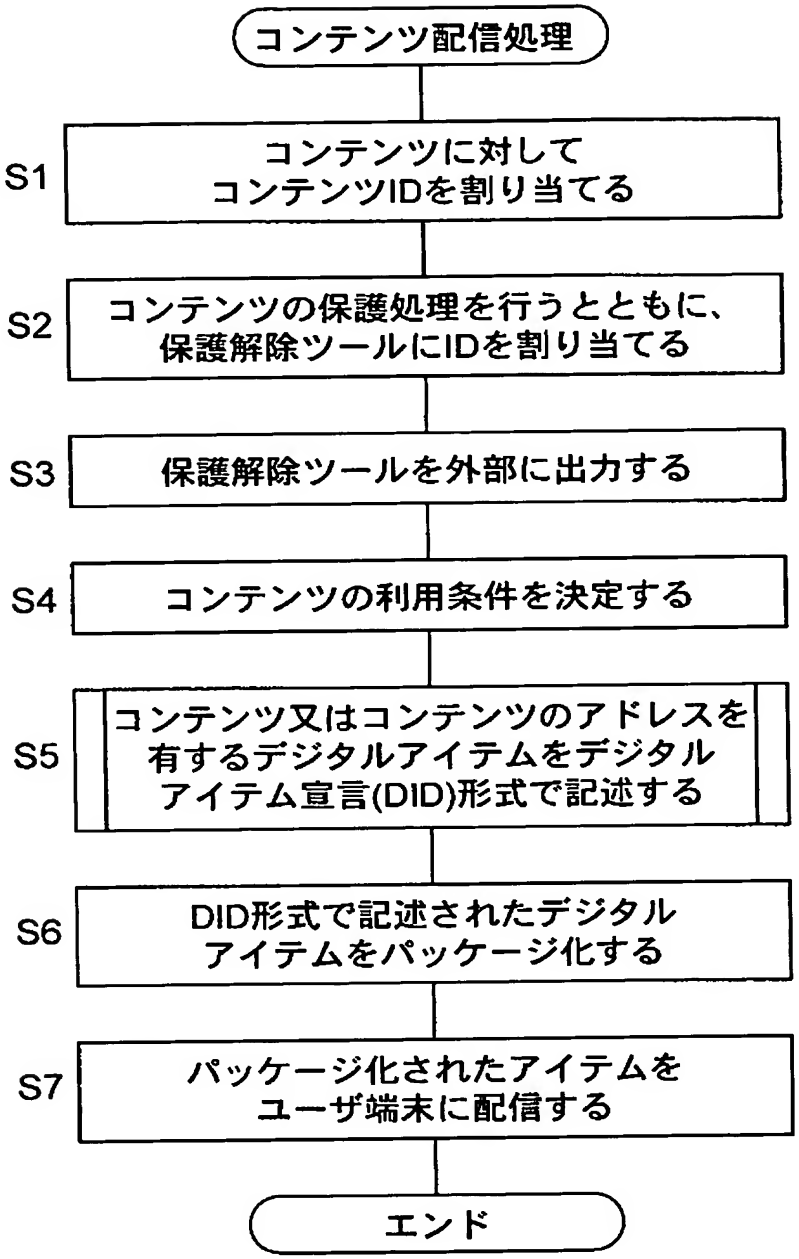
[図2]


イベントエンジン
イベント報告
信頼されるドメイン
ユーザセッション
ユーザプレファレンス
ユーザ選択動作/DI
IPMPユーザセッションマネジャ
2.1
2.6
RELエンジン
条件
2.5
条件を選択する
条件を調整する
条件を満たす
条件プロセッサ
2.8
DIPプロセッサ/DIME
2.10
DIXO
2.9
DIBO
メディアリソースの復号およびレンダリング
ルート信頼コンテキスト
認証原理
権利の行使
ユーザセッション状態更新状態
2.3
DIインスタンス
保証書
持続状態
2.4
ライセンスマネジャ
2.2
DIマネジャ
ユーザ認証子
ライセンスアクワイアラ
信頼されるドメイン2
セッション?
適応エンジン
DIアクワイアラ

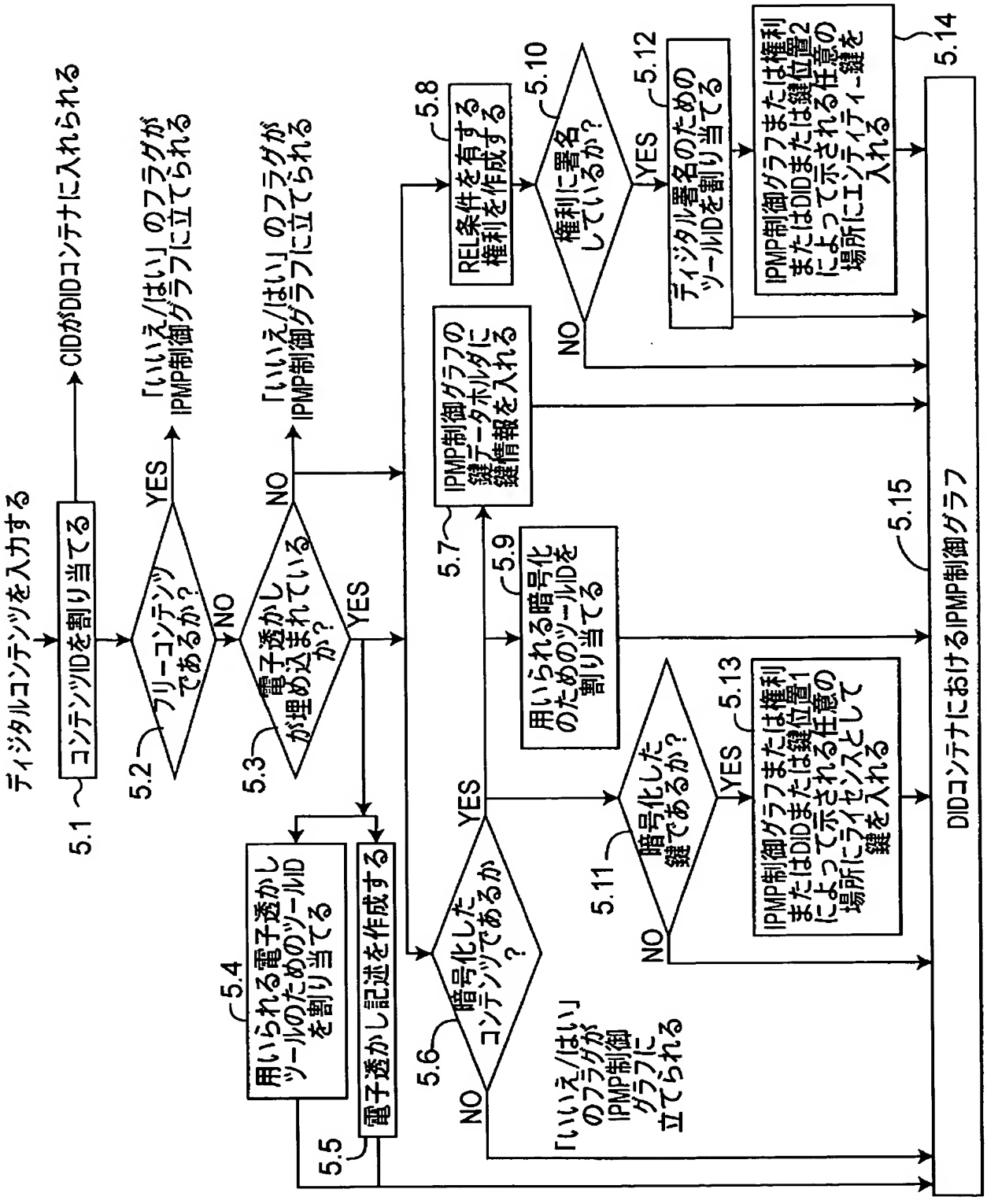
[図3]


20
配信部
28
パッケージング部
27
D-D記録部
26
コンテンツ保護処理部
24
利用条件データ生成部
25
コンテンツID割り当て部
23
インタフェース部
22

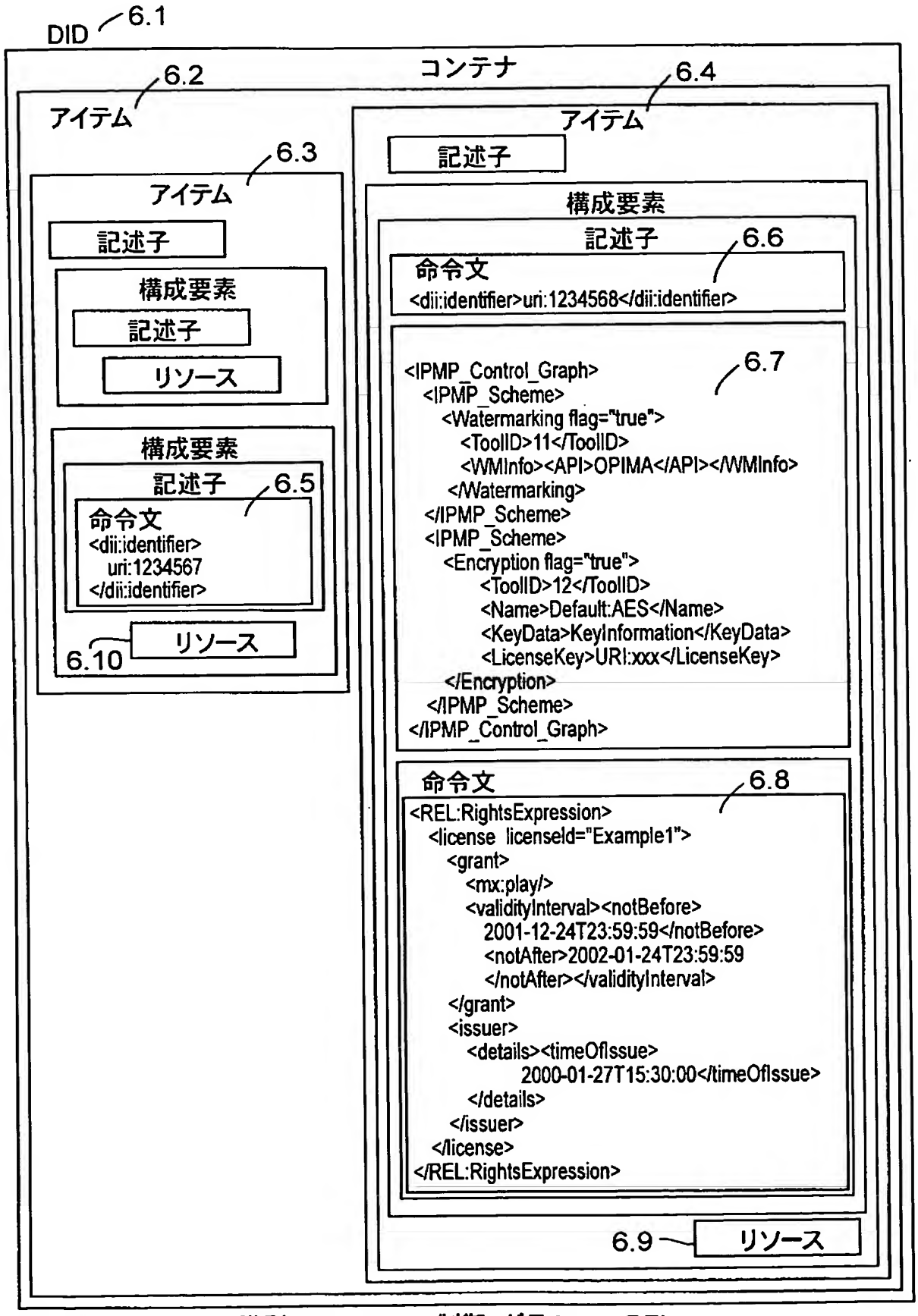
[図4]


コンテンツ配信処理
S1
コンテンツに対して
コンテンツIDを割り当てる
S2
コンテンツの保護処理を行うとともに、
保護解除ツールにIDを割り当てる
S3
保護解除ツールを外部に出力する
S4
コンテンツの利用条件を決定する
S5
コンテンツ又はコンテンツのアドレスを
有するデジタルアイテムをデジタル
アイテム宣言(DID)形式で記述する
S6
DID形式で記述されたデジタル
アイテムをパッケージ化する
S7
パッケージ化されたアイテムを
ユーザ端末に配信する
エンド

[図5]

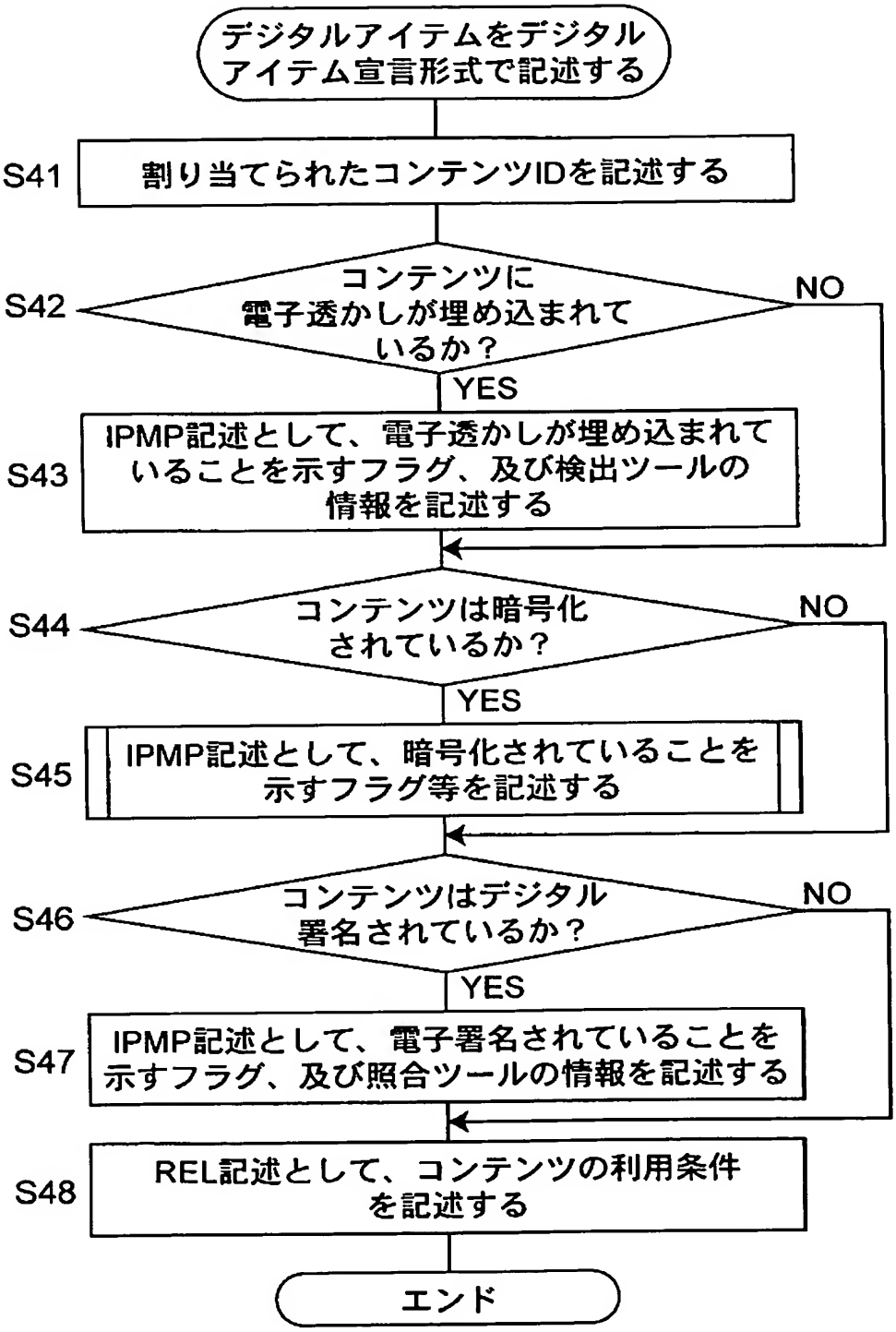

ディジタルコンテンツを入力する
5.1
コンテンツIDを割り当てる
CIDがDIDコンテナに入れられる
5.2
フリーコンテンツであるか?
YES
「いいえ/はい」のフラグがIPMP制御グラフに立てられる
NO
5.3
電子透かしが埋め込まれているか?
「いいえ/はい」のフラグがIPMP制御グラフに立てられる
NO
YES
5.4
用いられる電子透かしツールのためのツールIDを割り当てる
5.5
電子透かし記述を作成する
5.6
暗号化したコンテンツであるか?
YES
NO
「いいえ/はい」のフラグがIPMP制御グラフに立てられる
5.7
IPMP制御グラフの鍵データホルダに鍵情報を入れる
5.8
REL条件を有する権利を作成する
5.9
用いられる暗号化のためのツールIDを割り当てる
5.10
権利に署名しているか?
YES
NO
5.11
暗号化した鍵であるか?
YES
NO
5.12
ディジタル署名のためのツールIDを割り当てる
5.13
IPMP制御グラフまたは権利またはDIDまたは鍵位置1によって示される任意の場所にライセンスとして鍵を入れる
IPMP制御グラフまたは権利またはDIDまたは鍵位置2によって示される任意の場所にエンティティー鍵を入れる
5.14
5.15
DIDコンテナにおけるIPMP制御グラフ

[図6]

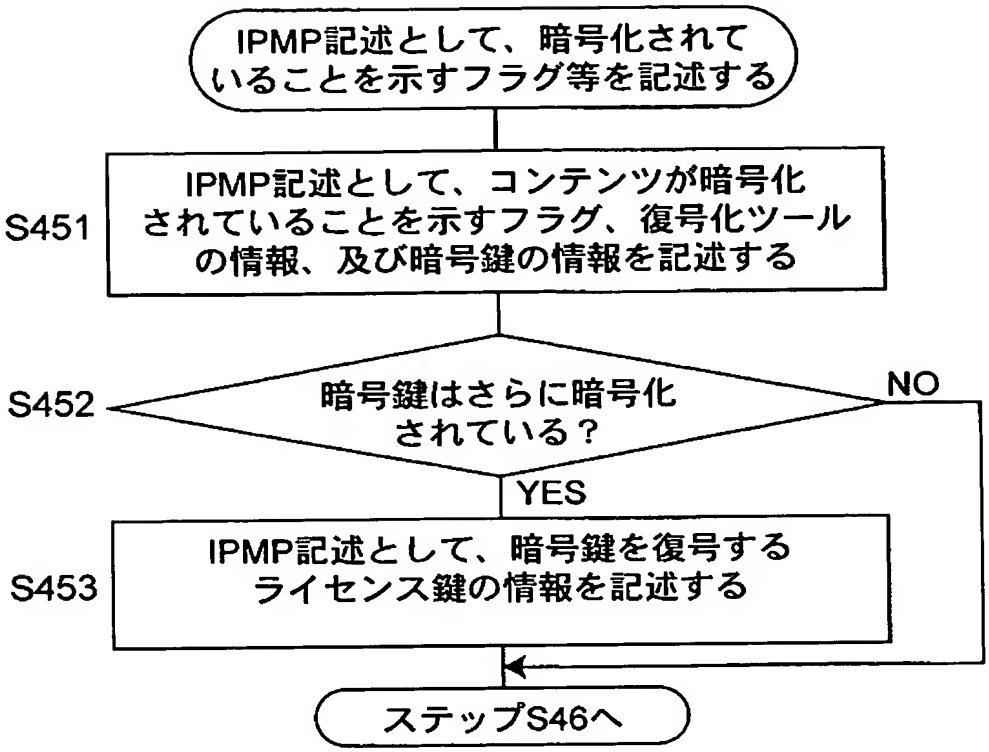


ディジタルアイテム識別(DII) IPMP_制御_グラフ REL

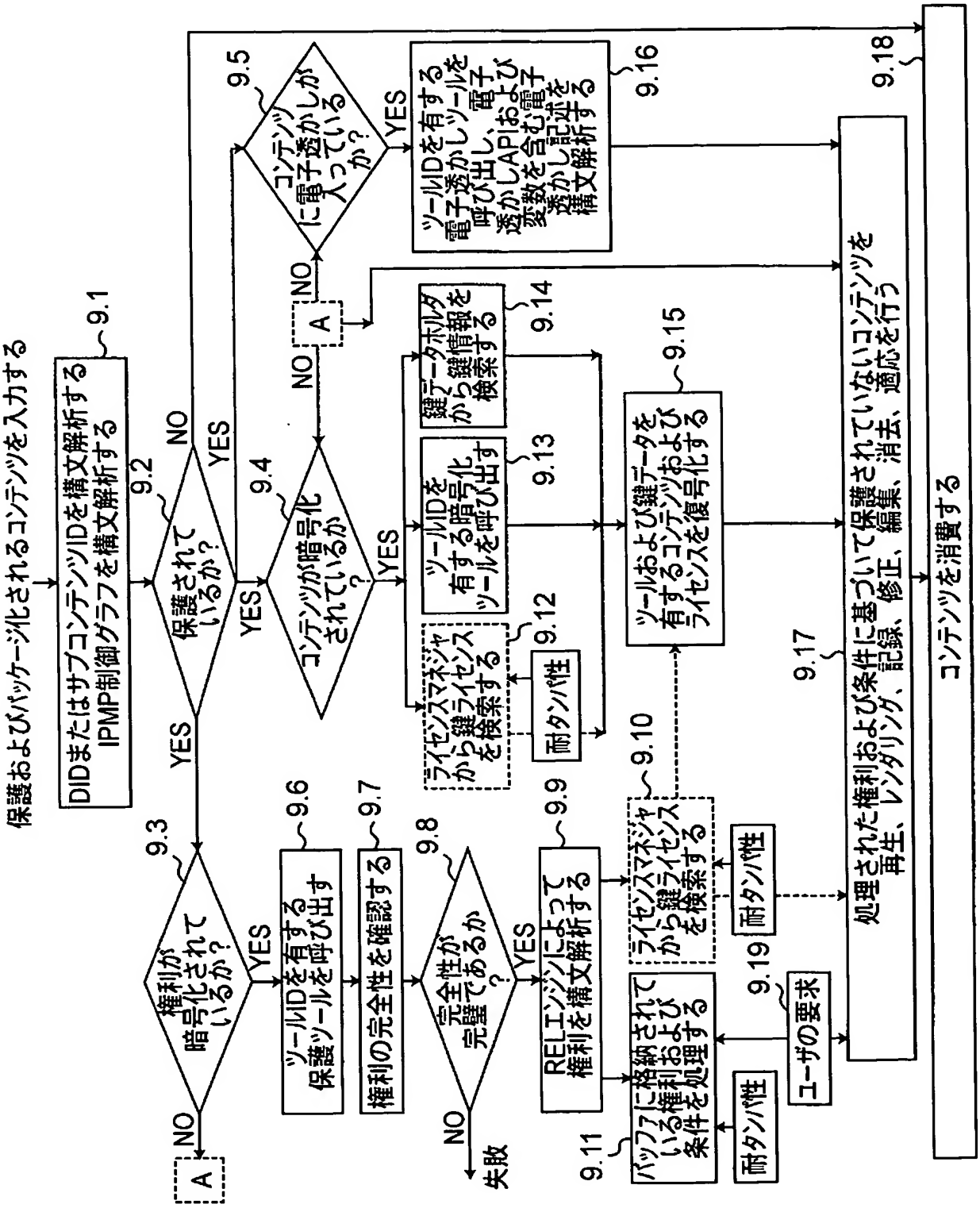
[図7]


デジタルアイテムをデジタルアイテム宣言形式で記述する
S41
割り当てられたコンテンツIDを記述する
S42
コンテンツに電子透かしが埋め込まれているか？
NO
YES
S43
IPMP記述として、電子透かしが埋め込まれていることを示すフラグ、及び検出ツールの情報を記述する
S44
コンテンツは暗号化されているか？
NO
YES
S45
IPMP記述として、暗号化されていることを示すフラグ等を記述する
S46
コンテンツはデジタル署名されているか？
NO
YES
S47
IPMP記述として、電子署名されていることを示すフラグ、及び照合ツールの情報を記述する
S48
REL記述として、コンテンツの利用条件を記述する
エンド

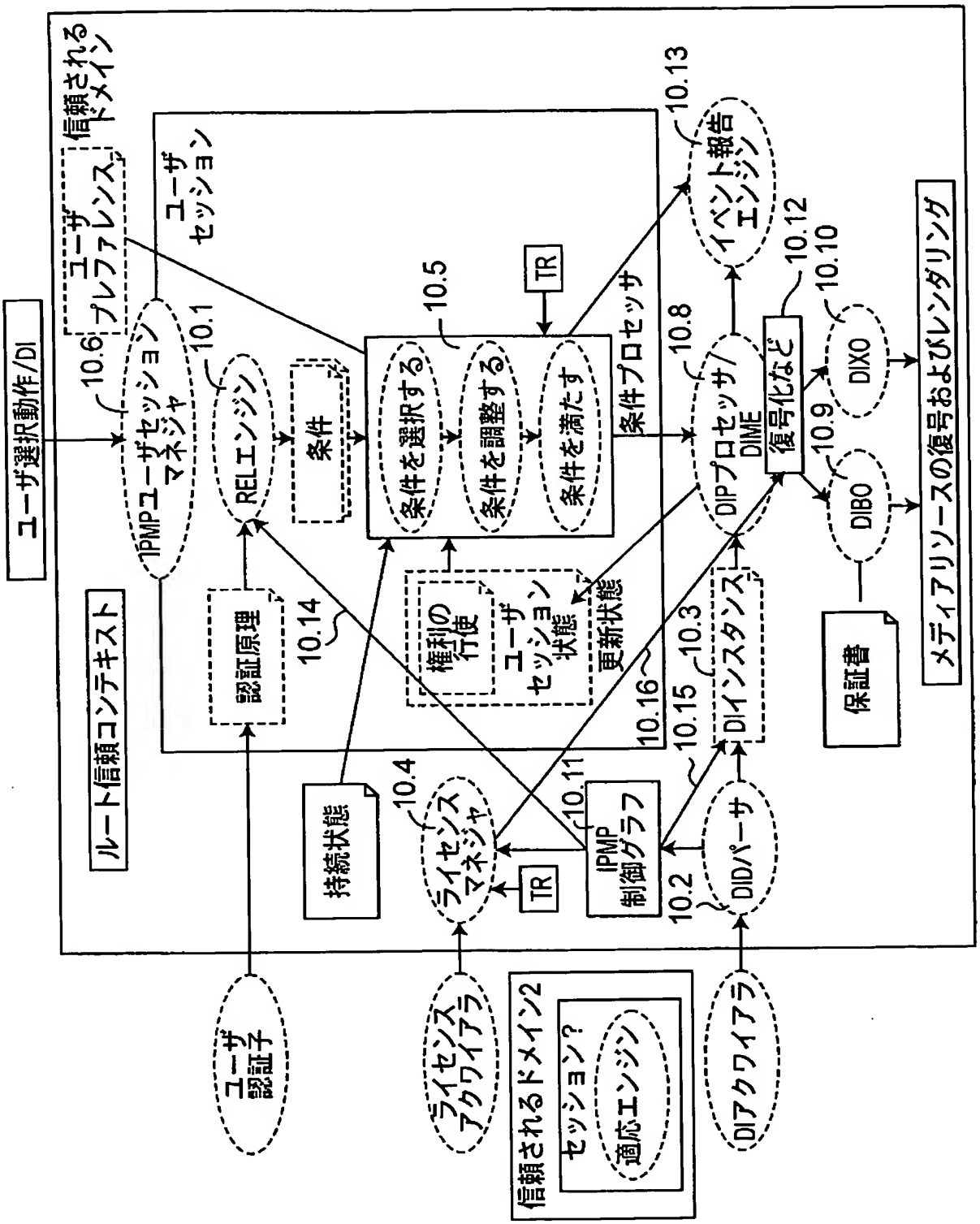
[図8]


IPMP記述として、暗号化されて
いることを示すフラグ等を記述する
S451
IPMP記述として、コンテンツが暗号化
されていることを示すフラグ、復号化ツール
の情報、及び暗号鍵の情報を記述する
S452
暗号鍵はさらに暗号化
されている？
NO
YES
S453
IPMP記述として、暗号鍵を復号する
ライセンス鍵の情報を記述する
ステップS46へ

[図9]

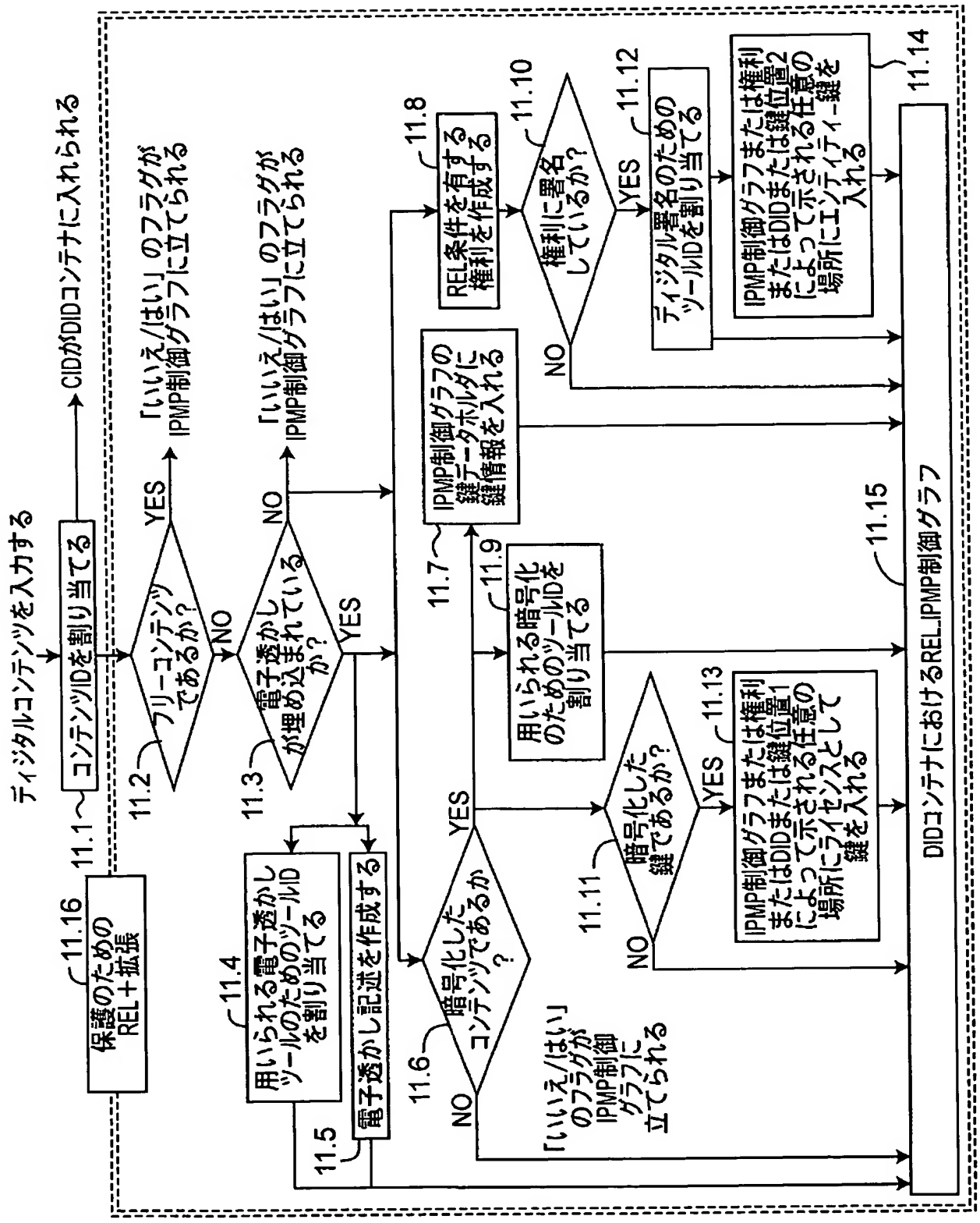

保護およびパッケージ化されるコンテンツを入力する
DIDまたはサブコンテンツIDを構文解析する IPMP制御グラフを構文解析する
9.1
保護されているか?
9.2
NO
YES
YES
コンテンツが暗号化されているか?
9.4
NO
YES
コンテンツに電子透かしが入っているか?
9.5
NO
YES
A
ツールIDを有する電子透かしツールを呼び出し、電子透かしAPIおよび変数を含む電子透かし記述を構文解析する
9.16
鍵データホルダから鍵情報を検索する
9.14
ツールIDを有する暗号化ツールを呼び出す
9.13
ライセンスマネジャから鍵ライセンスを検索する
9.12
耐タンパ性
ツールおよび鍵データを有するコンテンツおよびライセンスを復号化する
9.15
処理された権利および条件に基づいて保護されていないコンテンツを再生、レンダリング、記録、修正、編集、消去、適応を行う
9.17
9.18
コンテンツを消費する
権利が暗号化されているか?
9.3
YES
NO
A
ツールIDを有する保護ツールを呼び出す
9.6
権利の完全性を確認する
9.7
完全性が完璧であるか?
9.8
YES
NO
失敗
RELエンジンによって権利を構文解析する
9.9
ライセンスマネジャから鍵ライセンスを検索する
9.10
耐タンパ性
バッファに格納されている権利および条件を処理する
9.11
耐タンパ性
9.19
ユーザの要求

[図10]

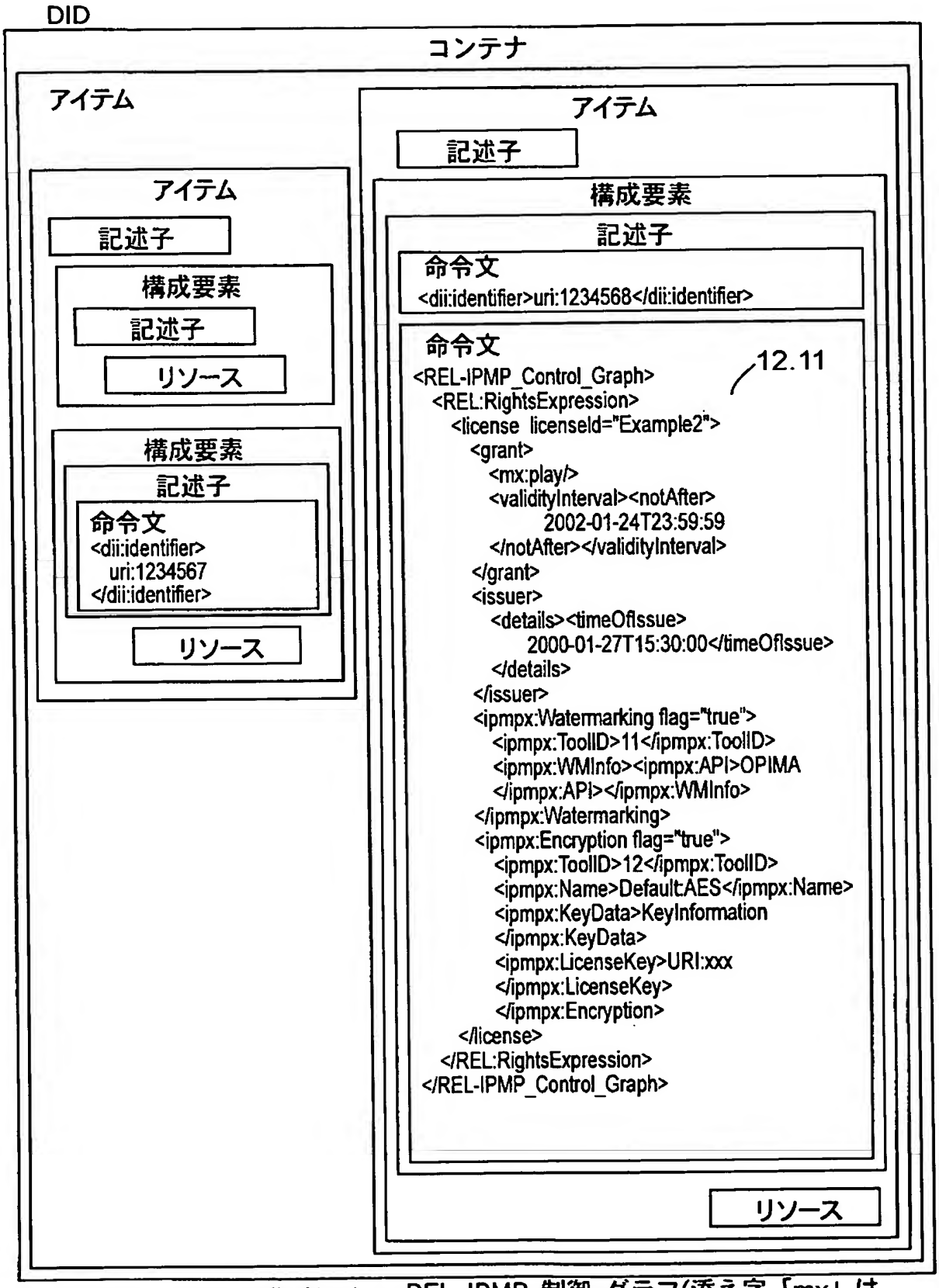

信頼されるドメイン
ユーザプレファレンス
10.6
ユーザセッション
ユーザ選択動作/DI
IPMPユーザセッションマネジャ
10.1
RELエンジン
条件
10.5
条件を選択する
条件を調整する
条件を満たす
TR
条件プロセッサ
10.8
イベント報告エンジン
10.13
DIPプロセッサ/DIME
復号化など
10.12
DIXO
10.10
DIBO
10.9
メディアリソースの復号およびレンダリング
保証書
ルート信頼コンテキスト
認証原理
10.14
権利の行使
ユーザセッション状態更新状態
10.16
10.3
DIインスタンス
10.15
持続状態
10.4
ライセンスマネジャ
TR
10.11
IPMP制御グラフ
10.2
DIDパーサ
ユーザ認証子
ライセンスアクワイアラ
信頼されるドメイン2
セッション?
適応エンジン
DIアクワイアラ

WO 2005/036407 PCT/JP2004/014344

[図11]



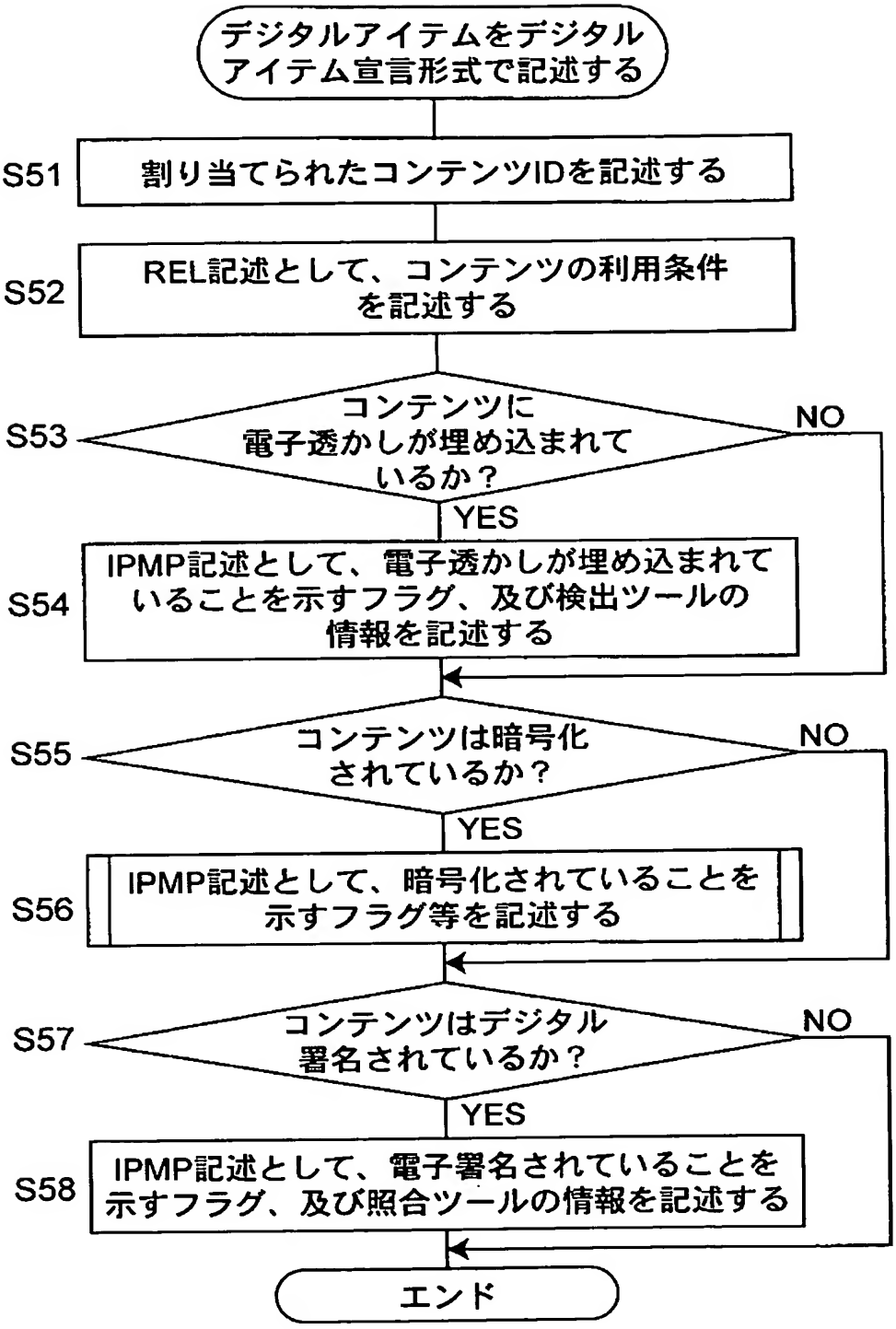
[図12]



ディジタルアイテム識別(DII)

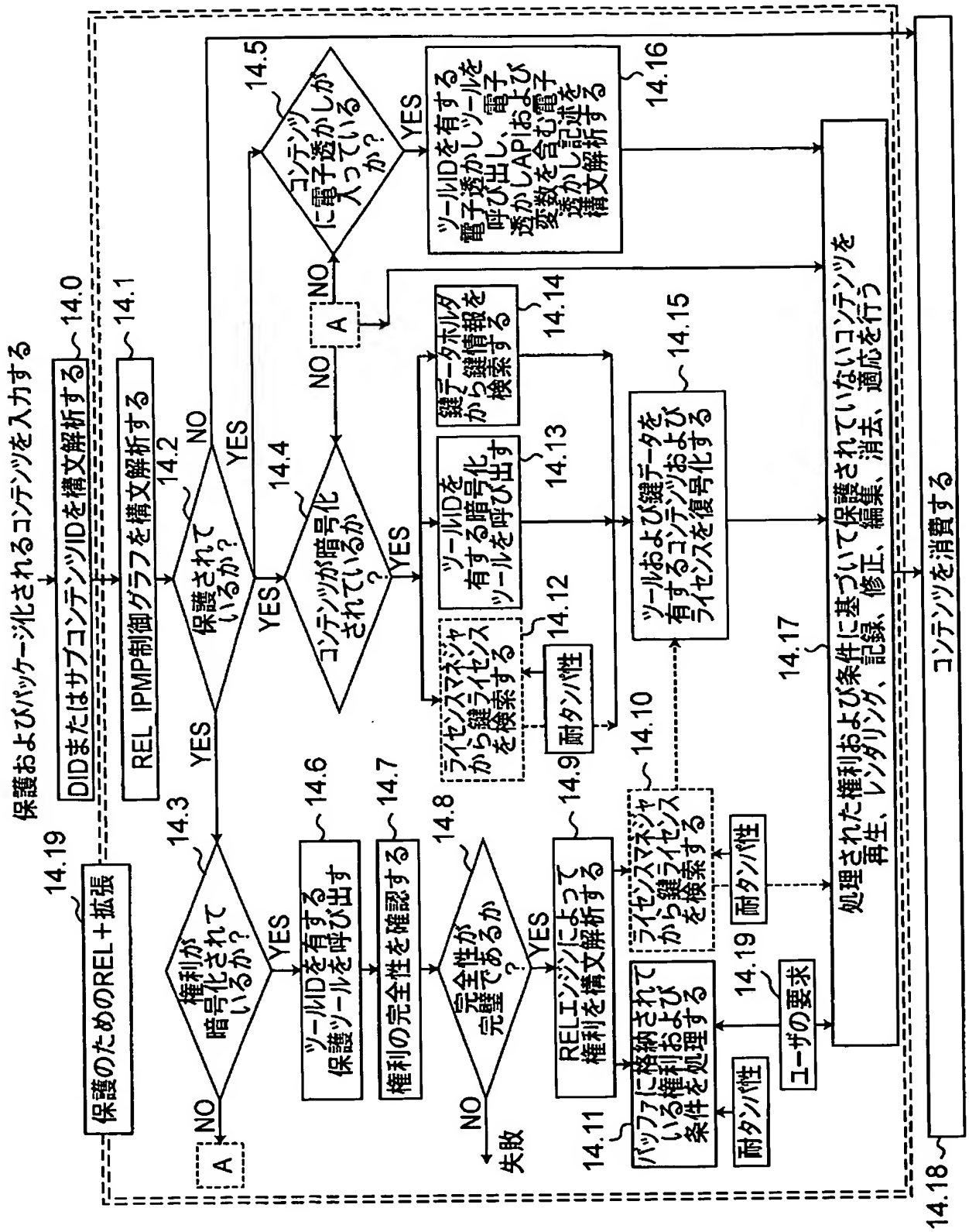
REL_IPMP_制御_グラフ(添え字「mx」はRELマルチメディア拡張を表し、「ipmpx」はREL IPMP拡張を表す)

[図13]

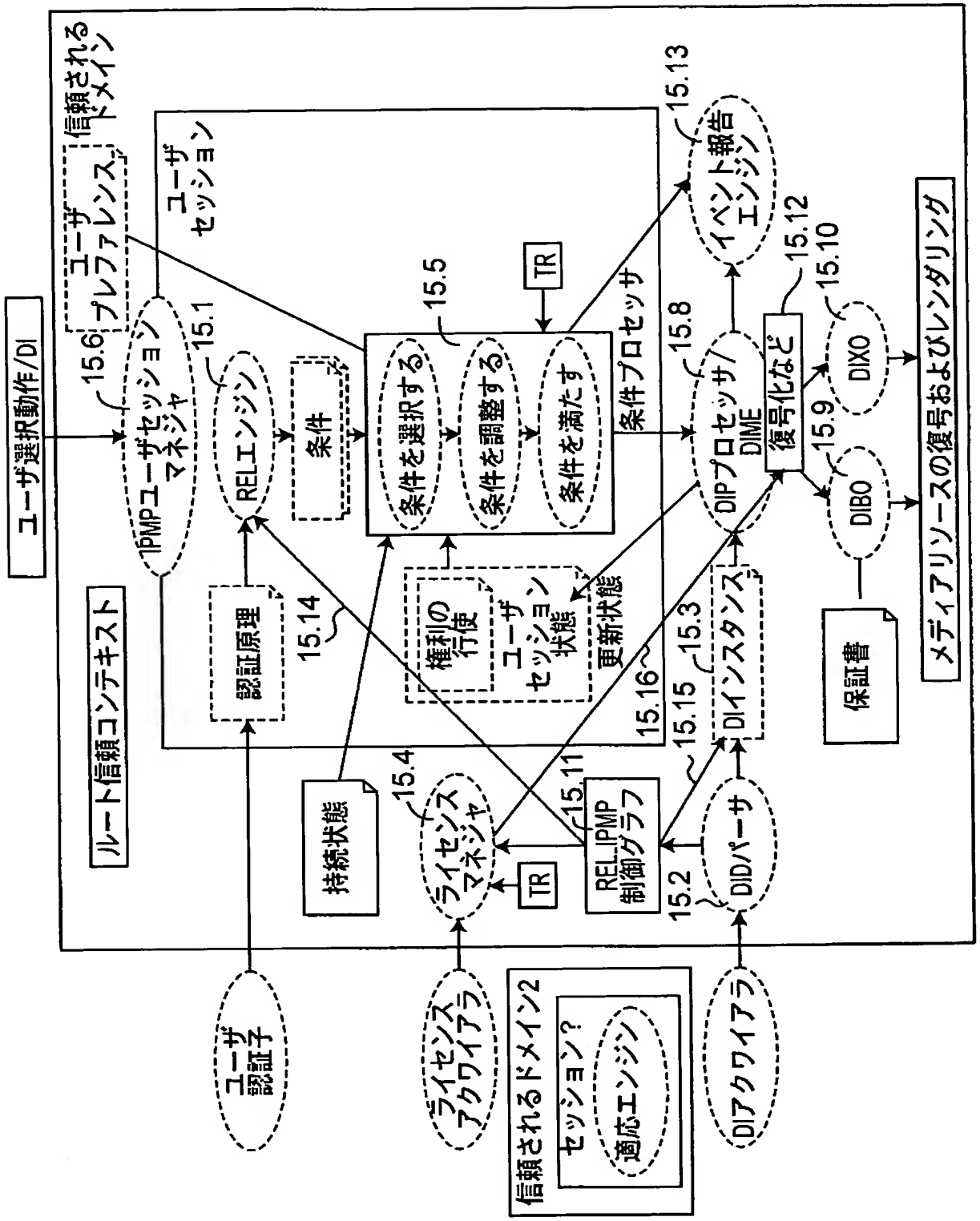

デジタルアイテムをデジタルアイテム宣言形式で記述する
S51
割り当てられたコンテンツIDを記述する
S52
REL記述として、コンテンツの利用条件を記述する
S53
コンテンツに電子透かしが埋め込まれているか？
NO
YES
S54
IPMP記述として、電子透かしが埋め込まれていることを示すフラグ、及び検出ツールの情報を記述する
S55
コンテンツは暗号化されているか？
NO
YES
S56
IPMP記述として、暗号化されていることを示すフラグ等を記述する
S57
コンテンツはデジタル署名されているか？
NO
YES
S58
IPMP記述として、電子署名されていることを示すフラグ、及び照合ツールの情報を記述する
エンド

WO 2005/036407 PCT/JP2004/014344

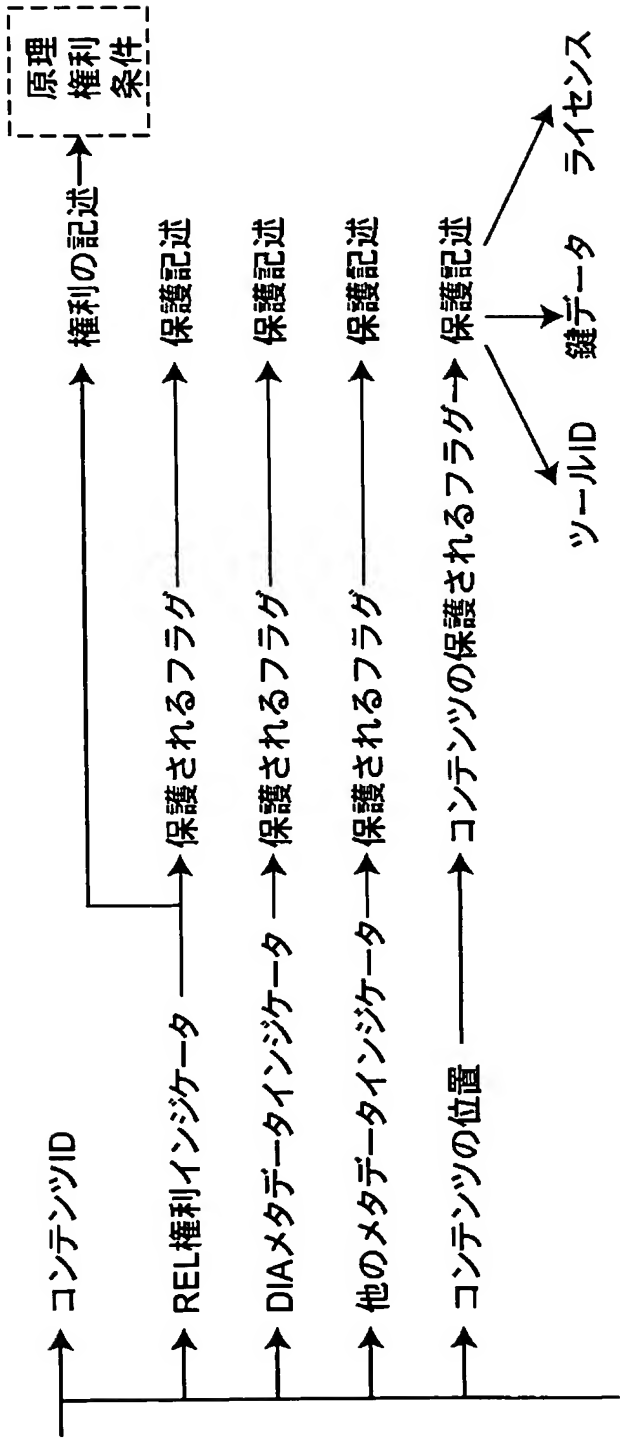
[図14]



[図15]


ユーザ選択動作/DI
信頼されるドメイン
ユーザプレファレンス
15.6
ユーザセッション
IPMPユーザセッションマネジャ
15.1
RELエンジン
条件
15.5
条件を選択する
条件を調整する
条件を満たす
条件プロセッサ
TR
15.13
イベント報告エンジン
15.12
15.10
DIXO
15.8
DIPプロセッサ/DIME
復号化など
15.9
DIBO
ルート信頼コンテキスト
認証原理
15.14
権利の行使
ユーザセッション状態更新状態
15.16
15.3
DIインスタンス
保証書
メディアリソースの復号およびレンダリング
持続状態
15.4
ライセンスマネジャ
TR
15.11
REL IPMP制御グラフ
15.15
15.2
DIDパーサ
ユーザ認証子
ライセンスアクワイアラ
信頼されるドメイン2
セッション?適応エンジン
DIアクワイアラ

[図16]


原理
権利
条件
権利の記述
コンテンツID
REL権利インジケータ
DIAメタデータインジケータ
他のメタデータインジケータ
コンテンツの位置
保護されるフラグ
保護されるフラグ
保護されるフラグ
コンテンツの保護されるフラグ
保護記述
保護記述
保護記述
保護記述
ツールID
鍵データ
ライセンス

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/014344

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/14, G06F15/00, G06F17/60, H04N1/387, H04N7/173

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/14, G06F15/00, G06F17/60, H04N1/387, H04N7/173

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Toroku Jitsuyo Shinan Koho	1994-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Supervised by Wataru KAMEYAMA, Tsuyoshi HANAMURA, "Digital Hoso Kyokasho (Ge)", Kabushiki Kaisha IDG Japan, 01 February, 2003 (01.02.03), pages 199 to 231	1-10
Y	Supervised by Hiroshi FUJIWARA, Hiroshi YASUDA, "Hyojun MPEG Kyokasho", Ascii Corp., 11 February, 2003 (11.02.03), pages 215 to 254	1-10
Y	JP 2003-199063 A (Matsushita Electric Industrial Co., Ltd.), 11 July, 2003 (11.07.03), All pages; all drawings; particularly, Par. Nos. [0051] to [0053] & WO 2003/015416 A1 & US 2004/93337 A1	1-10

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 28 December, 2004 (28.12.04)	Date of mailing of the international search report 25 January, 2005 (25.01.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

国際調査報告

国際出願番号 PCT／JP2004／014344

A. 発明の属する分野の分類（国際特許分類（IPC））
Int.Cl.[7] G06F12/14, G06F15/00, G06F17/60, H04N1/387, H04N7/173

B. 調査を行った分野
調査を行った最小限資料（国際特許分類（IPC））
Int.Cl.[7] G06F12/14, G06F15/00, G06F17/60, H04N1/387, H04N7/173

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報 1922－1996年
日本国公開実用新案公報 1971－2004年
日本国実用新案登録公報 1996－2004年
日本国登録実用新案公報 1994－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	亀山 渉, 花村 剛 監修, “ディジタル放送教科書（下）”, 株式会社ＩＤＧジャパン, 2003.02.01, pp.199-231	1-10
Y	藤原 洋, 安田 浩 監修, “標準ＭＰＥＧ教科書”, 株式会社アスキー, 2003.02.11, pp.215-254	1-10
Y	JP 2003-199063 A (松下電器産業株式会社) 2003.07.11, 全頁, 全図, 特に【００５１】－【００５３】段落 & WO 2003/015416 A1 & US 2004/93337 A1	1-10

☐ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
28.12.2004	25.1.2005

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	5N	3044
日本国特許庁（ISA／JP） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	髙橋 克 電話番号 ０３－３５８１－１１０１ 内線 ３５８５		

様式PCT／ISA／210（第2ページ）（2004年1月）